



**UNODC**

United Nations Office on Drugs and Crime



# Handbook on Identity-related Crime



UNITED NATIONS OFFICE ON DRUGS AND CRIME  
Vienna

# Handbook on Identity-related Crime



UNITED NATIONS  
New York, 2011

© United Nations, April 2011. All rights reserved.

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

This publication has not been formally edited.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

## Foreword

The present Handbook follows the release in 2007 of the United Nations study on “fraud and the criminal misuse and falsification of identity”, commissioned by UNODC and submitted to the United Nations Commission on Crime Prevention and Criminal Justice at its sixteenth session (E/CN.15/2007/8 and Add. 1-3), in line with Economic and Social Council resolution 2004/26. The main contribution and achievement of that study was two-fold: first, it adopted a broad approach on the concept of “identity-related crime” and considered it in an inclusive manner to cover all forms of illicit conduct involving identity, including offences described, often not consistently, as “identity fraud” and “identity theft”. Second, it dealt with the problems posed by identity-related crime from a new criminal justice perspective and the treatment of identity abuses as distinct criminal offences, as opposed to the traditional approach of criminalizing other activities committed using false identities. The study also tackled differences and deviations in definitional and conceptual approaches at the national level with regard to the criminal misuse and falsification of identity and shed light on various aspects revealing the complexity of the problem and its criminal diversity.

The Handbook builds upon the findings and recommendations of the abovementioned study and focuses on certain legal and policy issues pertaining to identity-related crime. Its main objective is to lay out a range of options and considerations to be taken into account when addressing domestic criminal justice matters (typology of crimes/criminalization approaches/protection of victims), specific challenges in the field of international cooperation in criminal matters or the potential of synergies and partnerships between the public and the private sector, mainly in the area of prevention of identity-related crime. The combination of both research papers and practice-oriented material serves the purpose of shedding light on different aspects and parameters of the complex problems posed by this form of crime.

Due to the diversity of the issues covered, the Handbook is destined for use by legislators, policy-makers, prosecution and law enforcement authorities and practitioners, as well as other stakeholders (representatives from international and intergovernmental organizations active in this field, representatives from the private sector and experts from academia).

It can also be used as resource material in technical assistance programmes and capacity-building activities with a view to increasing expert knowledge to address legal, institutional and operational issues around identity-related crime as an emerging form of crime, in line

with the policy directions provided by both the Bangkok and Salvador Declarations, outcomes of the Eleventh and Twelfth United Nations Congresses on Crime Prevention and Criminal Justice respectively.

In addition, the development of the Handbook as a technical assistance tool is a first effort to implement relevant mandates arising from ECOSOC resolutions 2004/26, 2007/20 and 2009/22 and calling for: (a) the use of the information gained by the abovementioned United Nations study for the purpose of developing useful practices, guidelines or other materials in the prevention, investigation and prosecution of the criminal misuse and falsification of identity; and (b) the collection, development and dissemination of more specific and thematically-oriented technical assistance material on identity-related crime, including manuals and compilations of useful practices or guidelines.

Lastly, the present Handbook benefited from the conclusions, guidelines and recommendations resulting from the meetings of a core group of experts on identity-related crime, established by UNODC in 2007 on a multi-stakeholder basis to bring together representatives from Member States and international organizations, as well as representatives from the private sector and experts from academia. The establishment of the core group has proved to be a successful initiative geared towards facilitating the exchange of views, information and expertise among those actors on the best course of strategic, policy and legal action against identity-related crime, as well as promoting their mutual understanding and cooperation to this effect.

## Acknowledgements

The present Handbook is the product of a project carried out by the Corruption and Economic Crime Branch of UNODC within its mandate arising from Economic and Social Council resolutions 2007/20 and 2009/22 on “International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime” and in line with its Thematic Programme on “Action against Corruption and Economic Crime” (2010-2011).

The elaboration of the Handbook also falls within the overall work of UNODC to develop new tools with the aim to assist Member States in strengthening their legal, institutional and operational capacities in order to combat economic fraud and identity-related crime at the domestic level, and to effectively engage in international cooperation to combat these crimes.

UNODC wishes to extend its thanks to the following experts who provided their substantive contributions to the drafting of this Handbook:

- Mr Marco Gercke, Lecturer for Law related to Cybercrime, University of Cologne, Germany;
- Mr Gilberto Martins de Almeida, Martins de Almeida Advogados, Rio de Janeiro, Brazil;
- Ms Philippa Lawson, Associate, International Centre for Criminal Law Reform and Criminal Justice Policy, Canada;
- Ms Raluca Simion, Legal Adviser, Directorate International Law and Judicial Cooperation, Ministry of Justice, Romania; and
- Mr Cormac Callanan, Managing Director, Aconite Internet Solutions Limited.

UNODC also acknowledges with profound gratitude the contribution of all those involved through their comments and feedback in this project, particularly the members of the core group of experts on identity-related crime, an initiative launched by UNODC in 2007 to pool experience from a wide range of stakeholders, develop strategies, facilitate further research and agree on practical action against identity-related crime.

UNODC avails itself of this opportunity to express its gratitude to the Government of Canada for its generosity in providing funding for the elaboration of the Handbook.

Mr Demosthenes Chryssikos, Crime Prevention and Criminal Justice Officer, Corruption and Economic Crime Branch, was the responsible UNODC officer for compiling and adapting the content of the Handbook.

Special thanks are due to Ms Dildora Djuraeva, contractor, for her substantive contribution to the accomplishment of this project.



# Contents

	<i>Page</i>
1. Legal Approaches to Criminalize Identity Theft <i>Marco Gercke</i> .....	1
2. Typology and criminalization approaches to identity-related crime: Compendium of examples of relevant legislation <i>Gilberto Martins de Almeida</i> .....	55
3. Identity-related crime victim issues: A Discussion Paper <i>Philippa Lawson</i> .....	107
4. Identity Theft: An inventory of best practices on public-private partnerships to prevent economic fraud and identity-related crime <i>Cormac Callanan</i> .....	169
5. Practical guide to international cooperation to combat identity-related crime <i>Marco Gercke/Raluca Simion</i> .....	235





# LEGAL APPROACHES TO CRIMINALIZE IDENTITY THEFT\*

**Marco Gercke**

**Lecturer for Law related to Cybercrime**

**University of Cologne, Germany**

---

\*The present study was prepared for use as working document at the third meeting of the core group of experts on identity-related crime, held in Vienna, Austria, on 20-22 January 2009. It was also submitted as a Conference Room Paper to the Commission on Crime Prevention and Criminal Justice at its eighteenth session, held in Vienna on 16-24 April 2009 (E/CN.15/2009/CRP.13). The opinions expressed in this paper are those of the author and do not reflect the views of the United Nations.



# Contents

	<i>Page</i>
I. SCOPE OF THE STUDY .....	5
1. The contours of the analysis .....	5
2. Aspects not covered by the study .....	5
II. OVERVIEW OF THE STRUCTURE.....	9
III. PHENOMENON.....	11
1. The transformation from personal interaction to the exchange of identity-related information .....	11
2. Identity-related information as a target .....	12
3. New methods of obtaining information as a result of the digitalization .....	15
4. Ways in which obtained information is used.....	19
5. Increased commission of computer-related identity theft and related challenges for investigations.....	21
IV. DEFINITION OF IDENTITY THEFT .....	25
1. General definitions .....	25
V. TYPOLOGY.....	31
1. Challenges related to the development of typology .....	31
2. Common principles .....	31
3. Relation to identity-related information, but no unifying act .....	33
VI. LEGAL APPROACHES.....	35
1. Arguments in favour of and against a specific identity theft offence .....	35
2. General concerns regarding the criminalization of identity theft.....	35
3. Applicability of traditional criminal law provisions .....	36
4. Precise definition of the object of legal protection.....	37
5. Practical aspects related to the investigation .....	37
6. Conflict between national and international dimensions .....	38
7. International approaches.....	38
8. National approaches .....	41
9. Essential elements of a legal approach .....	44
References .....	49





# I. SCOPE OF THE STUDY

## 1. The contours of the analysis

The study focuses on three major aspects of the legal response to identity theft. As described further in detail below, the term “identity theft” is used to describe a rather inhomogeneous field of offences.<sup>1</sup> Due to both the extent and the impact of the offences, the development of an adequate response to the threat is both challenging and necessary. This study does not intend to provide a comprehensive strategy addressing identity theft, but focuses on one piece of such strategy: the criminal law-based legal response.

## 2. Aspects not covered by the study

Various other elements of a comprehensive strategy against identity theft are not addressed in the present study, but are briefly mentioned below.

### *Preventive measures*

Different technical as well as legal measures have been developed to prevent identity theft. Such measures range from a restriction of the publication of critical identity-related information,<sup>2</sup> to data breach notification requirements<sup>3</sup> and a better protection of large databases.<sup>4</sup>

<sup>1</sup> See *infra*, chapter 4.

<sup>2</sup> See, in this context, Social Security Numbers, More could be done to protect SSNs, Statement of *C. M. Fagnoni*, Managing Director Education, Workforce and Income Security, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, 2006, GAO Document: GAO-06-586T, page 10 et seq.

<sup>3</sup> Notification requirements that oblige entities and institutions that experience a data breach to notify individuals whose personal information was affected by the incident. Regarding the Data Breach Notification Regime, see *Stevens*, Federal Information Security and Data Breach Notification Laws, 3 April 2008, CRS Report for Congress, Document RL34120; *Faulkner*, Hacking Into Data Breach Notification Laws, *Florida Law Review*, vol. 59, 2007, page 1097 et seq.; *Turner*, Towards a Rational Personal Data Breach Notification Regime, Information Policy Institute, June 2006; Recommendations for Identity Theft Related Data Breach Notification, Identity Theft Task Force, 19 September 2006, available at: [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf) (last visited October 2008); Privacy, Lessons Learned about Data Breach Notification, Report to Congressional Requesters, 2007, GAO Document: GAO-07-657; Social Security Numbers, More could be done to protect SSNs, *supra* n. 2, page 12 et seq. Regarding the discussion about the impact of data breach notification requirements on the prevention of Identity Theft, see *Romanosky/Relang/Acquisti*, Do Data Breach Disclosure Laws Reduce Identity Theft?, Seventh Workshop on the Economics of Information Security, Center for Digital Strategies, Tuck School of Business, available at: <http://weis2008.econinfosec.org/papers/Romanosky.pdf> (last visited October 2008); Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited. However, the full extent is unknown; Report to Congressional Requesters, 2007, GAO Document: GAO-07-737, page 32 et seq.

<sup>4</sup> Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of *G. C. Wilshusen*, Director, Information Security Issues, 2007, GAO Document: GAO-07\_935T, page 17.

### *Implementation of security measures*

The implementation of additional security measures such as PIN (Personal Identification Number) or biometric information<sup>5</sup> can help to prevent the abuse of more frequently exchanged identity-related personal information.<sup>6</sup>

### *Identity management solutions*

Technical measures concerning the management of identity-related information as well as strategies aiming to minimize the extent of identity-related information that are needed within e-commerce transactions can influence the risks of identity theft.<sup>7</sup>

### *Monitoring of user behaviour*

Technical solutions implemented to monitoring and analysing the usage of identity-related transactions can help to identify those being suspicious.<sup>8</sup>

### *Improvement of investigations*

Further progress can be achieved by improving investigation techniques, for example the interrogation of identity theft suspects.<sup>9</sup>

### *International cooperation*

Identity theft often has a transnational dimension.<sup>10</sup> This is especially relevant with regard to Internet scams.<sup>11</sup> In cases with a transnational dimension, the ability of national law

<sup>5</sup> See The Use of Technology to Combat Identity Theft, Report on the Study Conducted Pursuant to Section 157 on the Fair and Accurate Credit Transaction Act of 2003, 2005, available at: [https://www.treasury.gov/offices/domestic-finance/financial-institution/cip/biometrics\\_study.pdf](https://www.treasury.gov/offices/domestic-finance/financial-institution/cip/biometrics_study.pdf) (last visited October 2008).

<sup>6</sup> See *White/Fisher*, Assessing Our Knowledge of Identity Theft: The Challenge of Effective Prevention and Control Efforts, *Criminal Justice Policy Review* 2008, vol. 19, 2008, page 16 et seq. with further reference.

<sup>7</sup> Regarding Identity Management Strategies, see *Sury*, Identity-Management und Recht, *Informatik-Spektrum*, vol. 27, No. 3, 2004, page 287 et seq.

<sup>8</sup> Regarding the use of automatic fraud prevention screening systems, see Money Laundering, Extend of Money Laundering through Credit Card is Unknown, Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, United States Senate, 2002, GAO Document: GAO-02-670; on identity usage monitoring, see *Mashima/Ahamad*, Towards a User-Centric Identity-Usage Monitoring System, in Internet Monitoring and Protection, The Third International Conference, 2008, page 47 et seq.; *Fawcett/Provost*, Adaptive Fraud Detection, *Data Mining and Knowledge Discovery*, vol. 1, No. 3, 1997, page 291 et seq.; *Bolton/Hand*, Statistical Fraud Detection: A Review, 2002, available at: <http://metalab.uniten.edu.my/~abdrahim/ntl/Statistical%20Fraud%20Detection%20A%20Review.pdf> (last visited October 2008); Critical with regard to the related surveillance of the customer, see *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, *Bulletin of Science Technology Society*, 2007, vol. 27, 2008, page 11 et seq.; *Stoddart*, Who Watches the Watchers? Towards an Ethic or Surveillance in a Digital Age, *Studies in Christian Ethics*, 2008, vol. 21, 2008, page 363 et seq.

<sup>9</sup> In this context, see *Copes/Vieraitis/Jochum*, Bridging the Gap between Research and Practice: How Neutralization Theory can inform Reid Interrogations of Identity Thieves, *Journal of Criminal Justice Education*, vol. 18, No. 3, 2007, page 444 et seq.

<sup>10</sup> Results of the Second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, 2007 E/CN.15/2007/8/Add. 3, page 14; on the international cooperation in identity theft cases, see *Elston/Stein*, International Cooperation in Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf> (last visited October 2008).

<sup>11</sup> Regarding the transnational dimension of Cybercrime, see: *Keyser*, The Council of Europe Convention on Cyber-crime, *Journal of Transnational Law & Policy*, vol. 12, No. 2, page 289, available at: [http://www.law.fsu.edu/journals/transnational/vol12\\_2/keyser.pdf](http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf) (last visited October 2008); *Sofaer/Goodman*, Cyber Crime and Security—The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq., available at: [http://media.hoover.org/documents/0817999825\\_1.pdf](http://media.hoover.org/documents/0817999825_1.pdf) (last visited October 2008).



enforcement agencies to investigate is limited due to the principle of national sovereignty. This fundamental principle of international law restricts the authorization to carry out investigations in foreign territories.<sup>12</sup> International investigations therefore require cooperation from law enforcement agencies based on the legal frameworks for international cooperation.<sup>13</sup> An improvement in the means of cooperation can significantly increase the capacities to identify and prosecute offenders in transnational cases.

In case of identifying such a level of seriousness for offences targeting identity, Member States are provided with convincing and reliable arguments regarding the use of the United Nations Convention against Transnational Organized Crime (UNTOC) as a legal basis for international cooperation to combat those offences. As far as the other “enabling factors” for the application of the Convention are concerned, the transnational aspect seems to be in most cases an inherent element of identity-related crime, whereas the involvement of an organized criminal group is more or less implied where the means used to commit the crime are beyond the capabilities of individual offenders.<sup>14</sup>

### *Education*

The education of members of civil society about the risks related to the publication and unprotected use of identity-related information, as well as the strategies to protect against identity theft related offences, can decrease the risks of successful attacks.<sup>15</sup> This is especially relevant with regard to social engineering based scams such as “phishing”.<sup>16</sup>

### *Impact of identity theft*

Apart from the non-criminal law approaches, the study will not further analyze financial and criminology issues linked to identity theft. Therefore the impact, first of all, of identity theft will not further be developed. On this issue, it should be briefly mentioned that

<sup>12</sup> National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: <http://www.law.uga.edu/intl/roth.pdf> (last visited October 2008).

<sup>13</sup> Regarding the cooperation within transnational identity theft cases, see OECD Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, page 45. Regarding the need for international cooperation in the fight against Cybercrime, see *Punnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, Transnational Dimension of Cyber Crime and Terrorism, supra n. 11, page 35; *Sofaer/Goodman*, Cyber Crime and Security—The Transnational Dimension, *ibid*.

<sup>14</sup> The United Nations Convention against Transnational Organized Crime defines an organized criminal group as such if one of its objectives is to generate a “financial or other material benefit” (Article 2). Although identity-related crimes are not necessarily economic in nature, almost all of them fall within the scope of the Convention, as even non-economic identity-related offences are covered if they are linked to an organized criminal group that is also involved in economic crime. Moreover, the meaning of the term “financial or other material benefit” is relatively broad and includes, for example, trafficking in child pornography for reasons of sexual gratification. It therefore encompasses identity crimes where stolen or fabricated identification or identity information is treated as a form of illicit commodity and bought, sold or exchanged, as well as instances where identification is misused for personal or organizational gains, including non-financial gains such as securing entry into another country.

<sup>15</sup> See *White/Fisher*, Assessing Our Knowledge of Identity Theft..., supra n. 6, page 15 et seq.; *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003; OECD Scoping Paper on Online Identity Theft, supra n. 13, page 35.

<sup>16</sup> The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, *Computer und Recht*, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: <http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf> (last visited October 2008).

various studies analyze the economic impact of identity theft offences.<sup>17</sup> They indicate a loss of an estimated £1.3 billion to the British economy every year and a loss of more than US\$50 billion in the United States in 2005.<sup>18</sup> The majority of the studies highlight that identity theft is a serious challenge for societies as well as law enforcement agencies, not only in terms of the number of offences, but also in terms of the losses.<sup>19</sup> The main difficulties related to the interpretation of the studies is the fact that they are based on different definitions of identity theft and in general focus on single countries only.

One issue that needs to be taken into consideration in this context is the fact that the impact of identity theft is not limited to direct financial losses of the victim. The loss of reputation, losses caused to financial institutions, the cost of the work of law enforcement agencies and preventive measures need to be taken into consideration.<sup>20</sup>

### *Analysis of the victim's situation*

Victims issues in the field of identity theft is of great importance due to the fact that this crime has become a mass phenomenon with a wide range of possible impacts on the victim's situation.<sup>21</sup> A question that could be raised is who should be considered to be a victim: the financial institutions that very often cover the loss caused by economic crimes related to identity theft, and/or the person whose identity-related information was used?<sup>22</sup> The specific focus of the present study does not allow in-depth analysis of those issues (which are dealt with separately in the present Handbook).

<sup>17</sup> 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

<sup>18</sup> See Javelin Strategy and Research 2006 Identity Fraud Survey, Consumer Report, available at: <http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf> (last visited October 2008).

<sup>19</sup> See, for example, the studies mentioned supra, n. 17.

<sup>20</sup> Regarding the aspects that need to be taken into consideration to calculate the loss, see Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 10 et seq.; Personal Information, Data breaches are frequent, but evidence of resulting identity theft is limited..., supra n. 4, page 2; *White/Fisher*, Assessing Our Knowledge of Identity Theft..., supra n. 6, page 4.

<sup>21</sup> In this context, see OECD Scoping Paper on Online Identity Theft, supra n. 13, page 27.

<sup>22</sup> See Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, supra n. 20, page 11; Identity Theft, Available Data Indicate Growth in Prevalence and Cost, Statement of R. Stana, GAO Document: GAO-02-424T, 2002, page 5; *Levil/Burrows*, Measuring the Impact of Fraud in the United Kingdom, *British Journal of Criminology*, 2008, vol. 48, page 12; *Elston/Stein*, International Cooperation in Online Identity Theft Investigations..., supra n. 10, page 5.



## II. OVERVIEW OF THE STRUCTURE

The study is separated into three major parts. The first part<sup>23</sup> will analyze the phenomenon of those offences described by the term “identity theft”. It will further examine the type of identity-related information the offenders aim for, as well as the methods used for the commission of the offences. The analysis is the necessary basis to evaluate how far the different legal approaches address the phenomenon.

In the second part of the study,<sup>24</sup> existing approaches to define identity theft are considered, and, by taking into account the results of the analysis related to the phenomenon as well as the existing definition, a typology of identity theft is developed.

The third part of the study<sup>25</sup> provides an overview of arguments in favour and against the development of a specific approach to criminalize identity theft and highlights existing approaches. This part also presents potential elements which are necessary for the development of a national approach on the basis of the results of the first and second part of the study.

---

<sup>23</sup> See *infra*, chapter 3.

<sup>24</sup> See *infra*, chapters 4 and 5.

<sup>25</sup> See *infra*, chapter 6.



# III. PHENOMENON

## 1. The transformation from personal interaction to the exchange of identity-related information

Taking into account the wide media coverage,<sup>26</sup> the results of various surveys analysing the extent and loss caused by identity theft,<sup>27</sup> as well as numerous legal and technical analysis<sup>28</sup> that were published in the last years, identity theft seems to be a 21st-century phenomenon.<sup>29</sup> But this is not the case. Already in the 1980s the press reported about the misuse of identity-related information<sup>30</sup> and aspects related to identity theft, such as the fact that the falsification of documents in some countries is criminalized for more than a century.<sup>31</sup> What have changed are the scams the offenders use. While in the 1980s the classic mail theft played an important role, the increasing use of digital information has opened new possibilities for offenders to get rather easy access to identity-related information.<sup>32</sup> The transformation process from industrialized nations to information societies<sup>33</sup> had a great influence on the development of identity theft. But despite the large number of Internet-related identity theft cases, the digitalization did not enable the offence itself but created new targets and facilitated the development of new scams.<sup>34</sup>

<sup>26</sup> See, for example, *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: <http://edition.cnn.com/2006/US/05/18/identity.theft/> (last visited October 2008); Identity Fraud, *NY Times Topics*, available at: [http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity\\_fraud/index.html](http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html) (last visited October 2008); *Stone*, U.S. Congress Looks at Identity Theft, *International Herald Tribune*, 22.03.2007, available at: <http://www.iht.com/articles/2007/03/21/business/identity.php> (last visited October 2008).

<sup>27</sup> See supra n. 17.

<sup>28</sup> See, for example, *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, *Lex Electronica*, vol. 11, No. 1, 2006, available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited October 2008); *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, *MMR* 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: [http://www.privacyrights.org/ar/id\\_theft.htm](http://www.privacyrights.org/ar/id_theft.htm) (last visited October 2008).

<sup>29</sup> *Hoar*, Identity Theft: The Crime of the New Millennium, *Oregon Law Review*, vol. 80, 2001, page 1421 et seq.; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, vol. 49, 2008, page 8.

<sup>30</sup> See *Goodrich*, Identity Theft Awareness in North Central West Virginia, supra n. 15, page 1.

<sup>31</sup> See Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, page 5.

<sup>32</sup> *McCusker*, Transnational Organized Cybercrime: Distinguishing Threat From Reality, *Crime, Law and Social Change*, vol. 46, page 270.

<sup>33</sup> Unlike in the Industrial Society, members of the Information Society are no longer connected by their participation in industrialization, but through their access to and the use of ICTs. For more information on the information society see: *Masuda*, The Information Society as Post-Industrial Society, The Institute for Information Society, 1980; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe, Springer-Verlag, 2006; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society, Springer Science and Business Inc., 2005; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society, available at: <http://www.cils.org/WSIS/WSIS.htm> (last visited October 2008); *Hornby/Clarke*, Challenge and Change in the Information Society, Facet, 2003.

<sup>34</sup> *Clarke*, Technology, Criminology and Crime Science, *European Journal on Criminal Policy and Research*, vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, supra n. 20, page 51.

## 2. Identity-related information as a target

### *Increasing importance of identity-related information*

The reason for the relevance of identity theft in the 21st century is the growing importance of identity-related information in the economy as well as in social interaction. In the past, a “good name” and good personal relations dominated business as well as daily transaction.<sup>35</sup> With the transfer to electronic commerce, face-to-face identification was hardly possible, and, as a consequence, identity-related information became much more important for the participation in social and economic interaction.<sup>36</sup> This process can be described as instrumentalization,<sup>37</sup> whereby an identity is translated into quantifiable identity-related information is of great importance, as is the distinction between, on the one hand, identity of a person defined<sup>38</sup> as the collection of personal characteristics and, on the other, quantifiable identity-related information that enables the recognition of a person.

The requirements of non face-to-face transactions, such as trust and security<sup>39</sup> nowadays dominate the economy in general and not just e-commerce businesses. An example is the use of payment cards with a PIN (personal identification number) for purchasing goods in a supermarket where the PIN is not used to identify the customer, but as an indication for the legitimacy of the authorization of the payment.

### *Impact of the digitalization*

The digitalization and moreover the globalization of network-based services have led to an increasing use of identity-related information. Major parts of business as well as federal operations depend on the processing of electronic data by automated systems.<sup>40</sup> Having access to identity-related information enables the offenders to participate in wide areas of social life. Apart from this, the fact that this information is not only processed but in general also stored in databases makes those databases a potential target for offenders.

### *Traditional categories of data targeted by offenders*

The categories of identity-related information targeted by the offenders have changed as a consequence of the digitalization. Prior to the digitalization, the focus of the offender was on traditional identity-related information, such as passport number and information contained in birth certificates. The most common categories of such traditional identity-related information are:

<sup>35</sup> *Elston/Stein*, International Cooperation in Online Identity Theft Investigations..., supra n. 10, page 1.

<sup>36</sup> See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, *Datenschutz und Datensicherheit*, 2006, page 555.

<sup>37</sup> *Ceaton*, The Cultural Phenomenon of Identity Theft ..., supra n. 8, page 20.

<sup>38</sup> See *Encyclopaedia Britannica* 2007.

<sup>39</sup> *Halperin*, Identity as an Emerging Field of Study, *Datenschutz und Datensicherheit*, 2006, page 533.

<sup>40</sup> Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, supra n. 4, page 4.

## Social Security Number (SSN)

The SSN that is used in the United States is a classic example of a single identity-related data that perpetrators are aiming at. The Social Security Act of 1935 authorized the Social Security Administration to develop and maintain a record-keeping system to manage the Social Security programme.<sup>41</sup> Today the SSN is widely used by government entities in the United States to manage records, identify employees, as well as wage reporting and statistic purposes.<sup>42</sup> Yet it is not just governments which are using the SSN. The SSN is widely used by private businesses for identification purposes.<sup>43</sup> Information resellers, health care organizations and financial institutions use the SSN for internal matching purposes as well as for identifying existing or new customers.<sup>44</sup> Perpetrators can use the SSN as well as obtain passport information to open financial accounts, take over existing financial accounts, establish credit or run up debt.<sup>45</sup> With regard to identity theft, the major concern related to the SSN is the fact that it was not designed<sup>46</sup> to be used as an identification instrument and therefore does not include the necessary protection instruments required for identification instruments. Although the disclosure of a SSN by government entities was restricted under the Privacy Act of 1974,<sup>47</sup> recent identity theft cases highlight that the offenders were able to get access to SSN from public records.<sup>48</sup>

## Passport information

Passports are the main identification instruments in most countries.<sup>49</sup> They are used by government entities as well as private businesses to verify and identify people.<sup>50</sup> If the offenders manage to get access to the relevant passport information they can use that information to commit further offences.

## Driving licenses

Driving licenses can also be used for identification purposes.<sup>51</sup> It was reported that the hijackers of the 9/11 attack made use of a loophole in the legislation of the state of Virginia to obtain driving licenses by using fraudulent documents.<sup>52</sup>

<sup>41</sup> Social Security Numbers, More could be done to protect SSNs, Statement of *C. M. Fagnoni*, Managing Director Education, Workforce and Income Security, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, 2006, GAO Document: GAO-06-586T, page 3.

<sup>42</sup> *Ibid.*

<sup>43</sup> *Garfinkel*, Database Nation: The Death of Privacy in the 21st Century, O'Reilly, 2000, pages 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, *Harvard Journal of Law & Technology*, vol. 15, No. 2, 2002, page 350.

<sup>44</sup> *Supra* n. 41, page 8.

<sup>45</sup> See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: [http://www.privacyrights.org/ar/id\\_theft.htm](http://www.privacyrights.org/ar/id_theft.htm) (last visited October 2008).

<sup>46</sup> *Garfinkel*, Database nation..., *supra* n. 41.

<sup>47</sup> *Supra* n. 41.

<sup>48</sup> Social Security Numbers, Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate, GAO Document: GAO-07-752, 2007, page 1.

<sup>49</sup> *Wang/Chen/Atabakhsh*, Criminal Identity Deception and Deception Detection in Law Enforcement, *Group Decision and Negotiation*, vol. 13, 2004, page 119.

<sup>50</sup> *Stein*, Statement during the Hearing on the Role of Social Security Numbers (SSNs) in Identity Theft and Issues related to Enhancing Privacy, 2006, page 6, available at: <http://www.bits.org/downloads/Testimony/SteinTestimonyMar06.pdf> (last visited October 2008)

<sup>51</sup> *Supra* n. 49.

<sup>52</sup> *Elston/Stein*, International Cooperation in Online Identity Theft Investigations..., *supra* n. 11, page 4; on the use of false identities by the 9/11 terrorists, see *Wang/Chen/Atabakhsh*, Criminal Identity Deception..., *supra* n. 49.

## Financial account information and credit card numbers

Like the SSN, information regarding financial accounts is a popular target for identity theft.<sup>53</sup> This includes checking and saving accounts, credit cards, debit cards and financial planning information. Such information is an important source for an identity thief to commit financial crimes.

## Birth certificates

One of the most well known identity theft offences that does not involve digital information is related to birth certificate applications in the United Kingdom.<sup>54</sup> By gathering information about a deceased child and using that information with a birth certificate application, it used to be relatively easy to obtain a birth certificate holding false identity-related information.<sup>55</sup>

## *New categories of identity-related information targeted by offenders*

As digitalization has not decreased the importance of the above mentioned identity-related information, this still remains in the focus of offenders.<sup>56</sup> With regard to this information, the main change initiated by the digitalization process is the way the identity-related information is obtained.<sup>57</sup> But the digitalization led to further changes as it increased the categories of identity-related information.<sup>58</sup> Today account information and passwords, e-mail addresses and IP-addresses have become as important for verification and identification in network operations as passports and SSN. The most common new categories of identity-related information in the focus of the offender are the following:

## Account information and passwords

Access control systems of network-based services such as e-mail, online banking or hosting services very often use passwords. As a consequence, obtaining passwords to online services has become an important aspect of identity theft related offences.<sup>59</sup> Obtaining account information not only enables the offender to use the related service and make online transactions, send out e-mails or sell goods on an auction platform, but might also

<sup>53</sup> See Identity Theft, Greater Awareness and Use of Existing Data Are Necessary, Report to the Honourable Sam Johnson, House of Representatives, GAO Document: GAO-02-766, 2002, page 9; *Emigh*, Online Identity Theft: Phishing Technologies, Chokeypoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, page 6.

<sup>54</sup> For further information, see: <http://www.aboutidentitytheft.co.uk/your-birth-certificate.html> (last visited October 2008).

<sup>55</sup> *Levi*, Combating Identity and Other Forms of Payment Fraud in the United Kingdom: An Analytical History, published in *McNally/Newman*, Perspectives on Identity Theft.

<sup>56</sup> See *Gercke*, Internet-related Identity Theft, 2007, available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf](http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf) (last visited October 2008).

<sup>57</sup> See *infra*, chapter 3.3.

<sup>58</sup> Regarding the typical categories of data used for identification, see Results of the second meeting of the Inter-governmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, *supra* n. 10, page 6.

<sup>59</sup> See *Shamah*, Password Theft: Rethinking an old crime in a new area, *Mich. Telecomm. Tech. Law Review*, vol. 12, 2006, page 335 et seq.



grant access to further services. This is especially relevant with regard to e-mail addresses that are often used as an identification instrument.<sup>60</sup>

### Mac-address and IP-address

In order to authenticate legitimate customers and users, operators are making use of individualized parameters such as IP-addresses<sup>61</sup> or MAC-addresses.<sup>62</sup> The offender can falsify the MAC-address<sup>63</sup> or get access to the victim's computer network to make use of his IP-address<sup>64</sup> in order to take over the victim's identity.

## 3. New methods of obtaining information as a result of the digitalization

Describing identity theft by defining the methods used to commit the crime brings major challenges.<sup>65</sup> There are various different methods that are summarized under the umbrella of the term "identity theft".<sup>66</sup> They range from classic mail theft<sup>67</sup> to highly sophisticated phishing attacks.<sup>68</sup>

### *Traditional scams*

The most common scams related to non-digital identity-related information are:

#### *Redirection of mail*

By redirecting the post sent to the victim, the offenders can get access to personal information sent via mail<sup>69</sup> and prevent the victim from detecting suspicious activities.<sup>70</sup>

<sup>60</sup> Regarding e-mail based identification, see: *Garfinkel*, E-mail-based identification and authentication: an alternative to PKI, *Security & Privacy*, vol. 1, issue 6, 2003, page 20 et seq.

<sup>61</sup> An IP-address (Internet Protocol Address) is a numerical identification assigned to a device participating in a computer network. Regarding the definition and function of IP-address see: Understanding IP Addressing, 3COM White Paper, 2001, available at: [http://www.3com.com/other/pdfs/infra/corpinfo/en\\_US/501302.pdf](http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf) (last visited October 2008).

<sup>62</sup> A MAC address (Media Access Control address) is a unique identifier assigned to network devices.

<sup>63</sup> Regarding the means of manipulation and the detection of such falsification, see *Wright*, Detecting Wireless LAN Mac Address Spoofing, 2003, available at: <http://forskningstnett.uninett.no/wlan/download/wlan-mac-spoof.pdf> (last visited October 2008); *Guo/Chiueh*, Sequence Number-Based MAC Address Spoof Detection, available at: <http://www.ecsl.cs.sunysb.edu/tr/TR182.pdf> (last visited October 2008).

<sup>64</sup> Regarding the difficulties in cybercrime investigations that include abused wireless networks, see *Kang*, Wireless Network Security—Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and Wireless Technologies: Security and Risk Factors, Australian Institute of Criminology, 2006, available at: <http://www.aic.gov.au/publications/tandi2/tandi329t.html> (last visited October 2008).

<sup>65</sup> See *infra*, chapter 3.5.

<sup>66</sup> For an overview about the different techniques used to commit the Identity Theft, see: Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series), 2007.

<sup>67</sup> In a 2003 survey, mail theft was named by 68 per cent of the participants as a top concern. See *Gayer*, Policing Privacy, Law Enforcement's Response to Identity Theft, CALPIRG Education Fund, 2003, page 10.

<sup>68</sup> For the semantics of the term "phishing", see *supra* n. 16 (referring to *Gercke*, Criminal Responsibility for Phishing and Identity Theft, *ibid.*); see also *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: <http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf> (last visited October 2008).

<sup>69</sup> For example, credit cards, passwords, account statements.

<sup>70</sup> See Techniques of Identity Theft, CIPPIC Working Paper, *supra* n. 66, page 6.

### *Mail theft/theft of sources of personal information*

With regard to the fact that many important documents are sent by post, access to these sources remains an important method of obtaining identity-related information.<sup>71</sup> Other potential targets of thefts which aim for identity-related information are wallets, passports, driving licenses, address books, calendars and other sources of personal information.<sup>72</sup>

### *Dumpster diving*

The term “dumpster diving” is used to describe the process of sorting through bins to search for documents containing identity-related information.<sup>73</sup>

### *Insider attacks*

The 2007 CSI Computer Crime and Security Survey<sup>74</sup> points out that more than 35 per cent of the respondents attribute more than 20 per cent of their organization’s losses to insiders. The results of the survey correspond with reports about employees obtaining thousands of credit reports and credit card information.<sup>75</sup> One of the reasons for the success of insider attacks is the fact that a lot of security measures are designed to prevent outside attacks.

### *Using publicly available information*

Public records contain a range of identity-related information.<sup>76</sup> By searching for identity-related information in such publications, the offender can generate information that they are able to use for criminal purposes.

### *Scams related to digital information*

As described above, the digitalization has extended the range of methods to obtain identity-related information. Targeting digital data that enable the use of computer technology in obtaining the information brings a number of advantages for the offender, and related difficulties of law enforcement agencies.<sup>77</sup> Computer and network technology enable the offenders to acquire large amounts of personal data by only investing minimal energy.<sup>78</sup> Currently the most common scams related to digital identity-related information are the following:

<sup>71</sup> In a 2003 survey, mail theft was named by 68 per cent of the participants as a top concerns. See *Gayer*, Policing Privacy, Law Enforcement’s Response to Identity Theft, 2003, page 10.

<sup>72</sup> *Ibid.*, page 11.

<sup>73</sup> See *Zaidi*, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada, *Loyola Consumer Law Review*, vol. 19, issue 2, 2007, page 101; *Gayer*, Policing Privacy..., supra n. 71; *Siegel*, Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age, *Penn State Law Review*, vol. 111, No. 3, page 784; Discussion Paper Identity Crime, Model Criminal Law Officers’ Committee, supra n. 31, page 6.

<sup>74</sup> The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of cyber-crime businesses. It is based on the responses of 494 computer security practitioners from in United States corporations, government agencies and financial institutions. The Survey is available at: <http://www.gocsi.com/> (last visited October 2008).

<sup>75</sup> The 2005 Identity Theft: Managing the Risk report is taking regard to an incident where an employee of a United States company that supplied banks with credit reports used confidential computer passwords to access and download the credit reports of over 30,000 consumers during a three year period. See 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: [http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20\(White%20paper\).pdf](http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf) (last visited October 2008); on the related risks see as well: *Goodrich*, Identity Theft Awareness in North Central West Virginia, supra n. 15, page 11.

<sup>76</sup> Social Security Numbers, Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate, GAO Document: GAO-07-752, 2007, page 1.

<sup>77</sup> Regarding those challenges, see below under chapter 3.5.

<sup>78</sup> *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, *Crime, Law and Social Change*, vol. 46, page 270; *Elston/Stein*, International Cooperation in Online Identity Theft Investigations..., supra n. 10, page 2; *Faulkner*, Hacking Into Data Breach Notification Laws, *Florida Law Review*, vol. 59, 2007, page 1089.

(a) *Skimming*

The manipulation of ATMs to obtain the victim's credit card information and access codes has become a major concern in recent times.<sup>79</sup>

(b) *Phishing/pharming*

"Phishing" describes acts that are carried out to make victims disclose personal/secret information by using social engineering<sup>80</sup> techniques.<sup>81</sup> It is not a new kind of offence, but for decades known as "larceny by tick".<sup>82</sup> Although there are different types of phishing attacks,<sup>83</sup> e-mail-based phishing attacks contain three major phases: in the first phase, offenders identify legitimate companies that are offering online services and communicating electronically with customers.<sup>84</sup> In the second phase, the offenders design websites resembling the legitimate websites ("spoofing sites") of the identified company. In order to direct users to spoofing sites offenders often send out e-mails resembling those from the legitimate company.<sup>85</sup> Another technique to direct the user to the spoofed website is manipulation of the DNS—called "pharming".<sup>86</sup> In the third phase, the offenders use the information disclosed by the victim to log on to the victim's accounts and commit offences such as the transfer of money, application for passports or new accounts, etc. The rising number of successful attacks proves the threat of phishing attacks.<sup>87</sup>

*Malware*

Offenders aiming at identity-related information are increasingly making use of malicious software to obtain confidential information such as passwords, credit card numbers and social security numbers.<sup>88</sup> By installing<sup>89</sup> small software tools on the victim's computer, the offender can intercept communications, log keyboard strokes and search for information on the victim's computer.

<sup>79</sup> See Techniques of Identity Theft, CIPPIC Working Paper, supra n. 66, page 9.

<sup>80</sup> Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: <http://www.securityfocus.com/infocus/1527> (last visited October 2008).

<sup>81</sup> The term "phishing" originally described the use of e-mails to "phish" for passwords, supra n. 16; Ollmann, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: <http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf> (last visited October 2008).

<sup>82</sup> See Epstein/Brown, Cybersecurity in the Payment Card Industry, *University of Chicago Law Review*, vol. 75, 2008, page 205.

<sup>83</sup> See Gonsalves, Phishers Snare Victims with VoIP, 2006, available at: <http://www.techweb.com/wire/security/186701001> (last visited October 2008).

<sup>84</sup> Regarding the different phases of phishing, see OECD Scoping Paper on Online Identity Theft, supra n. 13, page 18.

<sup>85</sup> "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organized crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see supra: Offenders have developed advanced techniques to prevent users from realizing that they are not on the genuine website. For an overview about what phishing mails and the related spoofing websites look like, see: [http://www.anti-phishing.org/phishing\\_archive/phishing\\_archive.html](http://www.anti-phishing.org/phishing_archive/phishing_archive.html) (last visited October 2008).

<sup>86</sup> For more details, see Techniques of Identity Theft, CIPPIC Working Paper, supra n. 66, page 15.

<sup>87</sup> In some phishing attacks, as many as 5 per cent of victims provided sensitive information on fake websites. See Dhamija/Tygar/Hearst, Why Phishing Works, available at: [http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf) (last visited October 2008), page 1, that refers to Loftness, Responding to "Phishing" Attacks, Glenbrook Partners, 2004.

<sup>88</sup> See "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 4 et seq., available at: [http://www.antiphishing.org/reports/APWG\\_CrimewareReport.pdf](http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf).

<sup>89</sup> Regarding the various installation processes, see "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 21 et seq., available at: [http://www.antiphishing.org/reports/APWG\\_CrimewareReport.pdf](http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf) (last visited October 2008).

### *Hacking*

The term “hacking” is used to describe the unlawful access to a computer system.<sup>90</sup> It is one of oldest computer-related crimes<sup>91</sup> and in recent years has become a mass phenomenon.<sup>92</sup> Apart from famous targets like NASA, the United States Airforce, the Pentagon, Yahoo, Google, eBay and the German Government,<sup>93</sup> the offenders are more and more intensively focusing on the computer systems of regular users. As soon as they have access to the computer system they can obtain identity-related information. In addition offenders can target computer systems that host large databases with identity-related information.<sup>94</sup>

### *Theft/otherwise obtaining of storage devices*

Theft is in general considered to be a traditional offence, but the theft of computer and especially storage devices to get access to stored identity-related information has a different focus. The offenders are not aiming for the value of the hardware but are more interested in the analysis of stored information.<sup>95</sup> Such approaches range from legitimately buying second-hand hardware, where in a large number of cases sensitive information has not been properly deleted, to the intentional theft of computer systems.<sup>96</sup> The 2007 CSI Computer Crime and Security Survey<sup>97</sup> shows that nearly 15 per cent of the losses of respondents with regard to computer-related offences were related to the theft of confidential data and mobile hardware.<sup>98</sup> Although it is questionable whether the theft of computer hardware is considered to be a computer-related offence, the statistic underlines the importance of physical methods to obtain identity-related data.<sup>99</sup>

Apart from theft, information can be obtained from the lost computer and storage devices. In the last years, various reports were published that dealt with incidents

<sup>90</sup> In the early years of IT development, the term “hacking” was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term “hacking” was often used to describe a constructive activity.

<sup>91</sup> See *Levy*, Hackers: heroes of the computer revolution, Dell. Pub., 1994; Hacking Offences, Australian Institute of Criminology, 2005, available at: <http://www.aic.gov.au/publications/htcb/htcb005.pdf> (last visited October 2008); *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, Routledge, 2001, page 61.

<sup>92</sup> See the statistics provided by HackerWatch. The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported, see *Biegel*, Beyond our Control? Confronting the Limits of our Legal System in the Age of Cyberspace, Massachusetts Institute of Technology, 2001, page 231 et seq., in the month of August 2007. Source: <http://www.hackerwatch.org>.

<sup>93</sup> For an overview of victims of hacking attacks, see: [http://en.wikipedia.org/wiki/Timeline\\_of\\_computer\\_security\\_hacker\\_history](http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history) (last visited October 2008); *Joyner/Lotriente*, Information Warfare as International Coercion: Elements of a Legal Framework, *European Journal of International Law*, 2002, No. 5, page 825 et seq.; Regarding the impact, see *Biegel*, Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et seq.

<sup>94</sup> See: Techniques of Identity Theft, CIPPIC Working Paper supra n. 66, page 19; Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, supra n. 4, page 11.

<sup>95</sup> *Ceaton*, The Cultural Phenomenon of Identity Theft..., supra n. 8, page 15.

<sup>96</sup> See in this context: Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited..., supra n. 3, page 19.

<sup>97</sup> The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of Cyber-crime businesses. It is based on the responses of 494 computer security practitioners in United States corporations, government agencies and financial institutions. The Survey is available at: [available at: http://www.gocsi.com/](http://www.gocsi.com/) (last visited October 2008).

<sup>98</sup> CSI Computer Crime and Security Survey 2007, page 15, available at: <http://www.gocsi.com/> (last visited October 2008).

<sup>99</sup> Regarding the definition of computer crimes and cybercrime, see *Hayden*, Cybercrime’s impact on Information security, Cybercrime and Security, IA-3, page 3; Hale, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, vol. 18, available at: <http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37> (last visited October 2008).

where storage devices with large databases containing identity-related information were lost.<sup>100</sup>

### *New methods of using publicly available information*

As highlighted above, offenders do not necessarily have to commit crimes in order to obtain identity-related information. Identity-related information is publicly available on a large scale.<sup>101</sup> For example, offenders can use search engines to find identity-related data. “Googlehacking” or “Googledorks” are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to computer security issues, as well as personal information that can be used in identity theft scams.<sup>102, 103</sup> Reports highlight the risks that can go along with the legal use of search engines for illegal purposes.<sup>104</sup> Even the popular file-sharing systems can be used to obtain identity-related information.<sup>105</sup>

A new phenomenon closely connected to the development of new Internet-related services which are based on user-generated content is that of the social networks.<sup>106</sup> Facebook and Myspace are examples of online services which were designed to enable the user to present his or herself and keep in touch with others.<sup>107</sup> The information made available by the users ranges from names and date of birth to sexual interests. By getting access to those networks, offenders can obtain identity-related information that was voluntarily made available by the users and use it for criminal purposes.<sup>108</sup>

## 4. Ways in which obtained information is used

The impact of digitalization on the ways identity-related information that was obtained by the offender is then used is less intensive compared to the impact on the methods of obtaining the information. The most common ways identity-related information is used are:

<sup>100</sup> Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; supra n. 3, page 19; Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, supra n. 4, page 7; *Levi/Burrows*, Measuring the Impact of Fraud in the United Kingdom, supra n. 22, page 3.

<sup>101</sup> Regarding the unintended publication of identity-related information in networks, see Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; supra n. 3, page 7.

<sup>102</sup> *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, Syngress Publishing Inc., 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, O'Reilly, 2006.

<sup>103</sup> *Ibid.*

<sup>104</sup> See *Noguchi*, Search engines lift cover of privacy, *The Washington Post*, 09.02.2004, available at: <http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/> (last visited October 2008).

<sup>105</sup> See Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: <http://oversight.house.gov/documents/20071017134802.pdf> (last visited October 2008).

<sup>106</sup> Regarding the privacy concerns related to those social networks, see *Hansen/Meissner* (ed.), Linking digital identities, page 8. An executive summary is available in English (pages 8-9). The report is available online at: <https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf> (last visited October 2008).

<sup>107</sup> Regarding the identity sharing behaviour in social networks, see *Stutzman*, An Evaluation of Identity-Sharing Behavior in Social Network Communities, available at: [http://www.ibiblio.org/fred/pubs/stutzman\\_pub4.pdf](http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf) (last visited October 2008).

<sup>108</sup> Regarding the risks of Identity Theft related to such social networks, see *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, 2005, page 73, available at: <http://wiki.cs.columbia.edu:8080/download/attachments/1979/Information+Revelation+and+Privacy+in+Online+Social+Networks-gross.pdf> (last visited October 2008). On the use of social networks to make phishing attacks more efficient, see *Jagatic/Johnson/Jakobsson/Menczer*, Social Phishing, 2005, available at: <http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf> (last visited October 2008).

*Committing economic crimes*

In most cases the access to identity-related data enables the perpetrator to commit further crimes.<sup>109</sup> The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal activities. They can for example take over existing financial accounts or create new accounts by using the victim's identity-related information and then make transfers or purchase goods by using these accounts.<sup>110</sup>

*Selling the information*

Another approach is to sell the data<sup>111</sup> that can then be used by other perpetrators. Credit card records are, for example, sold for up to US\$60.<sup>112</sup> In this context the motivation of the perpetrator is to generate direct profit without carrying out the offence for which the obtained data are required. Such information can then be used to fabricate sophisticated identity documents or exploit weaknesses in insurance schemes, deceiving or corrupting authorities, in order to obtain genuine documents, which could then be sold to others to commit offences such as illicit travel, illegal migration or other activities.<sup>113</sup>

*Hiding the identity*

Perpetrators can use the information they obtained to hide their real identity.<sup>114</sup> They can request and use identification instruments to mislead investigations, or use the victim's bank account to launder money. In addition, they can circumvent identification and terrorist prevention measures by using obtained identities. The Report of the Secretary-General of the United Nations on Recommendations for a Global Counter-Terrorism Strategy highlights the importance of developing tools to tackle identity theft in the fight against terrorism.<sup>115</sup>

The challenges related to the ability to hide the identity can be demonstrated by examining the importance of identification routines to prevent money laundering. A significant number of measures to counter money-laundering are based on the "know-your-customer" principle and therefore depend heavily on identity or identification elements. Money-laundering scams make use of information, communication and commercial technologies, which enable offenders to generate false identification information and further facilitate, through the use of such false identification, remote transfers aimed at concealing laundered assets.<sup>116</sup>

<sup>109</sup> Consumer Fraud and Identity Theft Complain Data, January–December 2005, Federal Trade Commission, 2006, page 3, available at: [www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf](http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf) (last visited October 2008).

<sup>110</sup> For more information on the different offences, see *supra* n. 109.

<sup>111</sup> *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, *Lex Electronica*, vol. 11, No. 1, 2006, page 17, available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited October 2008).

<sup>112</sup> See 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: [http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20\(White%20paper\).pdf](http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf) (last visited October 2008).

<sup>113</sup> See *supra* n. 10, paragraph 18.

<sup>114</sup> See, in this context, Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, *supra* n. 10, page 10.

<sup>115</sup> Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy, 27.04.2006, A/60/825, page 13.

<sup>116</sup> Regarding the relation between identity-related offences and money laundering, see *supra* n. 114, page 12.

## 5. Increased commission of computer-related identity theft and related challenges for investigations

As described above, the digitalization as well as the instrumentalization process have expanded the opportunities and methods of committing identity theft related offences. Today digital information is a key target for identity theft and in a large number of cases information technology is used to commit these crimes. The following aspects have supported this development:

### *Availability of large databases*

With regard to the extensive use of computer technology, nearly all government entities and businesses are generating identity-related information and store it in databases.<sup>117</sup> The reports about the loss and theft of databases containing identity-related information about millions of customers demonstrates the threat that centralized storage of identity-related information brings.<sup>118</sup>

### *Tendency towards storing more information*

Experts are currently criticizing the fact that more and more information about user activities on the Internet is being stored.<sup>119</sup> Examples range from the storage of search activities to the storage of traffic data in countries with data retention obligations.<sup>120</sup>

### *Ability to duplicate large databases in a short period of time*

Copying a large number of tangible documents requires physical access to the documents, time for the reproduction process and, in general, involves a loss of quality that makes it possible to determine that the document is not the original. Compared to the disadvantages of the physical copying process, the duplication of databases carries a number of advantages. If the databases are available online then physical access is not necessary. In addition, digital information can be copied in a rather short time and without a loss of quality.<sup>121</sup>

### *Publicly available identity-related information*

As highlighted above, identity-related information is available in networks on a large scale. By simply trawling through the social networks, offenders are able to gather data that can be used for offences related to identity theft.<sup>122</sup>

<sup>117</sup> Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, supra n. 4, page 4.

<sup>118</sup> Regarding reports about the loss and theft of large databases with identity-related information, see Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; supra n. 3, page 19; Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, supra n. 4, page 7; *Levi/Burrows*, Measuring the Impact of Fraud in the United Kingdom, supra n. 22, page 3.

<sup>119</sup> See, for example, the statement by Bruce Schneier at the RSA Conference 2008 in London, Heise News, 29.10.2008, available at: <http://www.heise.de/newsticker/meldung/118119> (last visited October 2008); see also in this context, Discussion Paper Identity Crime, Model Criminal Law Officers' Committee supra n. 31, page 8.

<sup>120</sup> Regarding The Data Retention Directive in the EU, see *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, *Chicago Journal of International Law*, 2007, vol. 8, No. 1, available at: [http://eprints.law.duke.edu/archive/00001602/01/8\\_Chi.\\_J.\\_Int'l\\_L.\\_233\\_\(2007\).pdf](http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf) (last visited October 2008); *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 2005, page 365 et seq.

<sup>121</sup> A similar development can be observed with regard to copyright violations. Digitalization has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitalization, copying a record or a video-tape always resulted in a degree of loss of quality. Nowadays it is possible to duplicate digital sources without loss of quality, and also, as a result, to duplicate any copy.

<sup>122</sup> Regarding the risks of identity theft related to such social networks, see *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, 2005, page 73, available at: <http://wiki.cs.columbia.edu:8080/download/attachments/1979/Information+Revelation+and+Privacy+in+Online+Social+Networks-gross.pdf> (last visited October 2008).

*Ability to make use of large resources*

A number of organized crime groups have access to a significant number of computer systems that they can use to carry out automated attacks.<sup>123</sup> An example of the use of a large number of computer systems to carry out an attack was the successful attack against government websites in Estonia.<sup>124</sup> Analysis of the attacks highlights that those attacks could have been committed by thousands of computers that were part of a so-called “botnet”.<sup>125</sup> Reports underline that those “botnets” are not only used to carry out attacks but also to commit crimes related to identity theft.<sup>126</sup>

*Ability to act globally*

As pointed out above, committing a cybercrime does not in general require the presence of the perpetrator at the place where the victim is based. A significant number of cybercrime offences therefore affect more than one country.<sup>127</sup> Offenders can try to avoid criminal proceedings by acting from countries with weak cybercrime legislation.<sup>128</sup> In order to effectively fight cybercrime, “safe havens” that would enable the offenders to hide their activities must be prevented.<sup>129</sup> Given that there currently exist no international legal standards in the fight against identity theft, a close cooperation between the different national law enforcement presents unique challenges.<sup>130</sup>

*Ability to make use of means of anonymous communication*

The Internet offers offenders the possibility to effectively conceal their identity. Two examples are the use of public Internet terminals<sup>131</sup> or anonymous remailer.<sup>132</sup> The identification of the offenders presents unique challenges in those cases.<sup>133</sup>

<sup>123</sup> See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: <http://www.gao.gov/new.items/d05231.pdf> (last visited October 2008).

<sup>124</sup> For more information on those attacks, see *Lewis*, Cyber Attacks Explained, 2007, available at: [http://www.csis.org/media/isis/pubs/070615\\_cyber\\_attacks.pdf](http://www.csis.org/media/isis/pubs/070615_cyber_attacks.pdf) (last visited October 2008); A cyber-riot, *The Economist*, 10.05.2007, available at: [http://www.economist.com/world/europe/PrinterFriendly.cfm?story\\_id=9163598](http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598) (last visited October 2008); Digital Fears Emerge After Data Siege in Estonia, *The New York Times*, 29.05.2007, available at: <http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print> (last visited October 2008).

<sup>125</sup> See *Toth*, Estonia under cyberattack, available at [http://www.cert.hu/dmddocuments/Estonia\\_attack2.pdf](http://www.cert.hu/dmddocuments/Estonia_attack2.pdf) (last visited October 2008).

<sup>126</sup> See IT worker charged with harvesting bots to commit ID theft, *Computer Fraud & Security*, December 2007, page 4.

<sup>127</sup> Regarding the extend of transnational attacks in the most damaging cyberattacks, see *Sofaer/Goodman*, Cyber Crime and Security, supra n. 11, page 7.

<sup>128</sup> Offences related to phishing are an example. Although most sites are stored in the United States (32 per cent), China (13 per cent), the Russian Federation (7 per cent) and the Republic of Korea (6 per cent) are following. Apart from the United States, none of them has yet signed and ratified Cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

<sup>129</sup> The issue was addressed by a number of international organizations. The United Nations General Assembly Resolution 55/63 points out: “States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies”. The full text of the Resolution is available at: [http://www.unodc.org/pdf/crime/a\\_res\\_55/res5563e.pdf](http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf) (last visited October 2008); The G8 10 Point Action plan highlights: “There must be no safe havens for those who abuse information technologies”.

<sup>130</sup> *Elston/Stein*, International Cooperation in Online Identity Theft Investigations..., supra n. 10, page 1.

<sup>131</sup> Regarding legislative approaches to require an identification prior to the use of public terminals, see Article 7 of the Italian Decree-Law No. 144. For more details, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, *Computer und Recht International*, 2006, page 94 et seq.

<sup>132</sup> See *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, Conference on Communications and Multimedia Security, 1999.

<sup>133</sup> See *Gercke*, The Challenge of Fighting Cybercrime, *Multimedia und Recht*, 2008, page 294; *Elston/Stein*, International Cooperation in Online Identity Theft Investigations... supra n. 10, page 11.



*Ease of manipulating digital information*

Identity theft related offences often accompany the falsification of the obtained information. Digital information can be copied not only quickly and without a loss of quality,<sup>134</sup> but also can be rather easily modified if no protection measures<sup>135</sup> have been undertaken.<sup>136</sup>

---

<sup>134</sup> Ibid.

<sup>135</sup> For example, the use of digital signatures.

<sup>136</sup> See, in this context, Discussion Paper Identity Crime, Model Criminal Law Officers' Committee supra n. 31, page 8.



# IV. DEFINITION OF IDENTITY THEFT

A diverse range of identity theft definitions exists in different jurisdictions.<sup>137</sup> Not even the term used to describe the phenomenon is used consistently. While most United States publications use the term “identity theft”, the term “identity fraud” is very popular in the United Kingdom.<sup>138</sup> Other terms used are for example “identity-related offences”, “phishing”, “account takeover” or “account hijacking”.

## 1. General definitions

### *Combining obtaining and using an identity*

“Identity theft [...] occurs when one person [...] obtains data or documents belonging to another—the victim—and then passes himself off as the victim.”<sup>139</sup> The definition contains two key elements—the object (data or documents belonging to another) and two acts that are both required in order to lead to a criminalization. The first act is obtaining the data.<sup>140</sup> In addition, the offender needs to pass himself off as the victim. As a consequence, neither the sole act of obtaining the information nor the act of obtaining the information in order to sell it is covered by the definition.

### *Punishable act where identity is either target or tool*

“Identity-related crime concerns all punishable activities that have identity as a target or a principal tool.”<sup>141</sup> This definition is a rather a broad approach. It neither specifies the object covered nor does it specify the criminalized acts. It was introduced in an approach to define a higher-level category that covers various identity-related offences such as

<sup>137</sup> See OECD Scoping Paper on Online Identity Theft, supra n. 13, Annex 1; Gercke, Internet-related Identity Theft, 2007, available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf](http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf) (last visited October 2008).

<sup>138</sup> Regarding the different country specific approaches to the definition, see Paget, Identity Theft, McAfee White Paper, page 15, 2007, available at: [http://www.mcafee.com/us/threat\\_center/white\\_paper.html](http://www.mcafee.com/us/threat_center/white_paper.html) (last visited October 2008); Mitchison/Wilikens/Breitenbach/Urry/Portesi, Identity Theft—A Discussion Paper, page 22, available at: <https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf> (last visited October 2008).

<sup>139</sup> Mitchison/Wilikens/Breitenbach/Urry/Portesi, Identity Theft—A Discussion Paper, supra.

<sup>140</sup> Regarding the criminalization of obtaining identity-related information, see infra, chapter 5.2.2.

<sup>141</sup> See Koops/Leenes, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 556.

identity theft and identity fraud.<sup>142</sup> This is also the approach followed in the United Nations study on “the criminal misuse and falsification of identity”.<sup>143</sup> In some contexts, the term “identity abuse” was also used with a similar meaning, but without carrying any implicit assumption about whether a given conduct is already a criminal offence or should be criminalized. Due to the broad approach, the definition is not suitable to develop a criminal law provision, however it is useful from a methodological point of view in order to take into account a range of conducts that need to be considered in developing concrete typologies and possibly undertaking legislative action on criminalization.

#### *Fraud or other unlawful activity where the identity is the target or tool*

“Identity ‘theft’ is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person’s consent.”<sup>144</sup> The term identity theft in this definition is very close to the previous one. It contains two key elements: the object (identity) and the related act (fraud or any unlawful activity). Neither the object, nor the acts are further described.

#### *Assumption of an identity*

“Identity ‘theft’ may be used to describe the theft or assumption of a pre-existing identity (or significant part of it), with or without consent, and regardless of whether the person is dead or alive.”<sup>145</sup> This definition again contains two elements: the object (identity) and the related act (assumption). Compared to other definitions, the current definition provides a more detailed description of the object. But the definition of the act focuses on obtaining the identity. Therefore, the transfer of identity-related information or the use of such information is not covered by the provision.

#### *Taking over a fictitious identity or adopting the name of a person*

“ID fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.”<sup>146</sup> The definition contains two elements: the object (fictitious or real identity) and the related act (taking over/adoption). Neither the object nor the acts are further defined. The provision concentrates on the act of obtaining the identity and—depending on the interpretation of “takes over”—the use of the identity. Therefore, it is unlikely that transferring or selling the identity-related information would be covered. One unique aspect is the fact that the definition does cover the act of taking over a fictitious name. At first sight, this approach seems to pose difficulties, since, for example, the famous British actor Richard Jenkins, who used the name “Richard Burton”, and likewise the famous American writer Truman Steckfus-Persons, who used

<sup>142</sup> Ibid.

<sup>143</sup> See supra n. 10, paragraph 4.

<sup>144</sup> Supra n. 141.

<sup>145</sup> *Paget*, Identity Theft, McAfee White Paper, page 5, 2007, available at: [http://www.mcafee.com/us/threat\\_center/white\\_paper.html](http://www.mcafee.com/us/threat_center/white_paper.html) (last visited October 2008).

<sup>146</sup> Identity Fraud: A Study, United Kingdom Cabinet Office, 2002, page 11, available at: <http://www.ips.gov.uk/identity/downloads/id-fraud-report.pdf> (last visited October 2008).

the name “Truman Capote”, would be committing a crime by using a pseudonym. However, the approach does take into account the fact that current research<sup>147</sup> highlights that the majority of identity theft offences are related to fictitious (synthetic) identities.<sup>148</sup> Another concern is that the focus of criminalization is limited to names. Other identity-related information is not included in the definition.

### *Definitions used in surveys*

A similar inconsistency exists in surveys that list and analyse identity theft related developments and therefore it is necessary to define the scope of the survey, for example:

#### *United States Federal Trade Commission*

The ‘Consumer Fraud and Identity Theft Complaint Data’ survey published by the United States Federal Trade Commissions contains information related to the definition of identity theft: “Credit card fraud (26 per cent) was the most common form of reported identity theft”.<sup>149</sup> In the context of the study concerning identity theft, the act of obtaining identity-related information (“theft”) was not separated from the criminal offence that is committed by using this information (credit card fraud).

#### *United Kingdom Fraud Advisory Panel*

The requirement of two acts can be found in a report published by the Fraud Advisory Panel. The study lists certain forms of identity theft—among them the following example: “The fraudster will obtain a certified copy of the victim’s birth certificate (which is both straightforward and lawful) and apply for identification documents on the basis of that birth certificate. Identification documents could include passports, driving licenses and national insurance.”<sup>150</sup> In this example, the offence requires two acts: obtaining and using identity-related information.

### *Legal definitions*

As discussed further in detail below, only a few states have so far decided to criminalize identity-related offences with a specific provision.<sup>151</sup> At the time of drafting the present study, the most well-known approaches of defining identity theft were adopted in the United States, while the enactment of ad hoc legislation on this issue was pending in Canada (at a later stage, Bill S-4 was adopted as an amendment to the Canadian Criminal Code (identity theft and related misconduct). The following is a brief delineation of the United States legislative approach:

<sup>147</sup> Discussion Paper Identity Crime, Model Criminal Law Officers’ Committee, supra n. 31, page 4 with reference to United States National Fraud Ring Analysis, ID Analytics, 2008.

<sup>148</sup> Regarding synthetic identities related identity theft scams, see: *McFadden*, Synthetic identity theft on the rise, *Yahoo Finance*, 16.05.2007, available at: <http://biz.yahoo.com/brn/070516/21861.html?.v=1>.

<sup>149</sup> Consumer Fraud and Identity Theft Complaint Data, January–December 2005, Federal Trade Commission, 2006, page 3, available at: [www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf](http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf) (last visited October 2008).

<sup>150</sup> See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: <http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf> (last visited October 2008).

<sup>151</sup> For an overview about identity theft legislation in Europe, see *Owen/Keats/Gill*, The Fight Against Identity Fraud..., supra n. 159; *Mitchison/Wilikens/Breitenbach/Urry/Portesi*, Identity Theft, supra n. 138; Legislative Approaches To Identity Theft..., supra n. 159; For an overview about the legislation in Australia, the United States and the United Kingdom, see Discussion Paper Identity Crime, Model Criminal Law Officers’ Committee, supra n. 31, 2007.

*18 U.S.C. § 1028*

Provision 18 U.S.C. § 1028(a)(7) defines identity theft as: “Knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.” This definition again contains three elements—the object (means of identification), the act (transfers, possesses, or uses) and the intention that links the acts to further criminal activities (intent to commit, or to aid or abet, or in connection with, any unlawful activity). In the case of both the acts, as well as the intended offences, the provision follows a broad approach. Unlike the way the term identity theft is used in the Consumer Fraud and Identity Theft Complaint Data survey, it is especially not mandatory with regard to § 1028(a)(7) that the act is related to fraud.

*15 U.S.C. 1681a*

Another description is provided by the United States Federal Trade Commission. A brief description of the term “identity theft” is contained in 15 U.S.C. 1681a(q)(3): “*Identity theft*—the term “identity theft” means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.” The main difference to the description provided by 18 U.S.C. § 1028(a)(7) is the fact that 15 U.S.C. 1681a(q)(3)—similar to the Consumer Fraud and Identity Theft Complaint Data survey—links the term identity theft to fraud. This limits the application of the provision in other cases where the offender is using the identity-related information for other offences. In addition, despite the fact that the provision defines an act that contains the word “theft”, it only criminalizes the use of the information but not the act of obtaining it.

Based on 15 U.S.C. 1681a(q)(3), the Federal Trade Commission provided a more detailed description of identity theft:<sup>152</sup>

- (a) The term “identity theft” means a fraud committed or attempted using the identifying information of another person without lawful authority.
- (b) The term “identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:
  - 1) Name, Social Security number, date of birth, official state- or government-issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.
  - 2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation.
  - 3) Unique electronic identification number, address, or routing code.
  - 4) Telecommunication identifying information or access device.

Like 15 U.S.C. 1681a(q)(3), the description links the term identity theft to fraud and only covers the act of using the identity-related information.

<sup>152</sup> Related Identity Theft Definitions, Duration of Active Duty Alerts, and Appropriate Proof of Identity Under the Fair Credit Reporting Act, Federal Register 69, No. 82.

### *Provisional result*

The definitions used to describe more precisely the covered acts show a great degree of diversity. With regard to the need for precision in drafting criminal law provisions, none of the general definitions and those used in surveys can be taken as a basis for the development of a legal response. Different criteria are responsible for the lack of precision. The different emphasis on the terms “identity theft” and “identity fraud” is just one visible sign of the problem.<sup>153</sup> One of the reasons is the fact that a number of the definitions have a tendency to be too broad.<sup>154</sup> Analysis of the use of the terms “identity theft” and “identity fraud” in the media as well as in surveys<sup>155</sup> shows that there is also a tendency to call traditional crimes like credit card fraud “identity theft”.<sup>156</sup> The United Nations Intergovernmental Expert Group to prepare a study on Fraud and the Criminal Misuse and Falsification of Identity in 2007 therefore suggested that the term “identity crime” and/or “identity-related crime” be used to cover the sub-categories “identity theft” and “identity fraud”.<sup>157</sup>

The general term “identity crime” is used to cover all forms of illicit conduct involving identity, including identity theft and identity fraud.<sup>158</sup> In this context the use of the component “crime” is very often more of an outlook as most states have not yet adopted legislation on such offences.<sup>159</sup> Identity crime includes preparatory or constituent offences such as forgery and impersonation. One problem in the definition is that identity abuses may target identity information itself or other information to which it is linked. The latter case might not be considered identity crime, although the effects of such crime would usually be the same.

The lack of a precise definition does not, in general, hinder the development of effective legal measures, as the overview of identity theft related legislation shows. However, two main consequences of the missing definition can be identified.<sup>160</sup> First, it is more difficult to identify the true extent of the problem as the diverse definitions make it complex to compare the results of surveys; and, second, without an agreement on basic principles, such as a definition, it is in general more difficult to come up with an international approach and coordinate international investigations. Common or converged definitional approaches are an important basis for international cooperation, including transborder evidence-sharing, extradition of offenders and mutual legal assistance.<sup>161</sup>

<sup>153</sup> See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, supra n. 141.

<sup>154</sup> *Levi*, Combating Identity and Other Forms of Payment Fraud in the United Kingdom..., supra n. 55.

<sup>155</sup> See, for example Consumer Fraud and Identity Theft Complaint Data, January–December 2005, Federal Trade Commission, 2006, page 3, available at: [www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf](http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf) (last visited October 2008).

<sup>156</sup> *Levi*, Combating Identity and Other Forms of Payment Fraud in the United Kingdom, supra n. 55.

<sup>157</sup> OECD Scoping Paper on Online Identity Theft, supra n. 13, page 60.

<sup>158</sup> Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, supra n. 10, page 4.

<sup>159</sup> For an overview about identity theft legislation in Europe, see *Owen/Keats/Gill*, The Fight Against Identity Fraud: A Brief Study of the EU, the United Kingdom, France, Germany, and the Netherlands, Perpetuity Research & Consultancy International, 2006; *Mitchison/Wilikens/Breitenbach/Urry/Portesi*, Identity Theft, supra n. 138; Legislative Approaches To Identity Theft: An Overview, CIPPIC Working Paper No. 3, 2007; For an overview about the legislation in Australia, the United States and the United Kingdom, see Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, supra n. 31, 2007. Regarding the criminalization in the OECD Member States, see OECD Scoping Paper on Online Identity Theft, supra n. 13.

<sup>160</sup> See *White/Fisher*, Assessing Our Knowledge of Identity Theft..., supra n. 6.

<sup>161</sup> Regarding the cooperation within transnational Identity Theft cases, see OECD Scoping Paper on Online Identity Theft, supra n. 13, page 45.





# V. TYPOLOGY

## 1. Challenges related to the development of typology

The overview of the phenomenon<sup>162</sup> of identity theft as well as the different definitions<sup>163</sup> demonstrate that very few common criteria exist. The ways in which identity-related information is obtained varies to a large extent. Common methods range from mail theft to highly sophisticated phishing scams. Taking into account the availability of identity-related information in social networks,<sup>164</sup> where it is voluntarily disclosed by the users, highlights that obtaining this information does not necessarily require illegal acts. A similar diversity can be observed with regard to the types of data that perpetrators aim for. They range from information such as the Social Security Number to e-mail addresses. Not even the motivation of the perpetrators to obtain information is consistent. While some perpetrators use the obtained information for criminal activities, others sell them or use them to mislead investigations.

## 2. Common principles

Despite the existing diversity, the overview of the phenomenon of identity theft as well as the definition show at least some overlapping that can be used to extract common principles to develop a typology.

### *Four main elements*

Definition of identity-related offences in general contain four different categories of elements: the object (identity-related information), the criminalized acts (ranging from obtaining information to the use), a mental element (ranging from knowledge to a special intent) and finally, the missing authorization by the victim. Those four elements are required for the development of a criminal law provision in defining the structure.

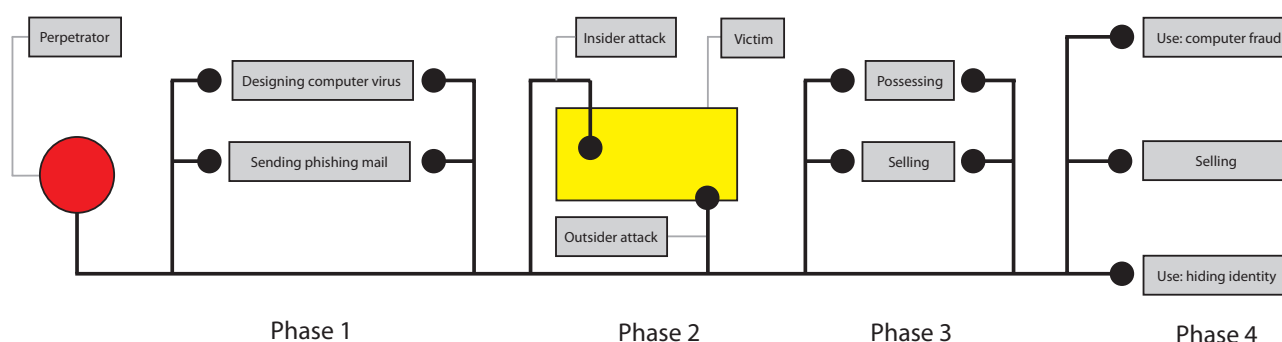
<sup>162</sup> See *supra*, chapter 3.

<sup>163</sup> See *supra*, chapter 4.

<sup>164</sup> Regarding the risks of identity theft related to such social networks, see *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, *supra* n. 122, page 73.

### *Distinction in four phases*

It is possible to make a distinction between four different phases in which identity-related offences can potentially take place:<sup>165</sup>



#### *Phase 1*

The first phase can be characterized as a preparation phase. Using the term preparation can be misleading as there is very often already an interaction with the victim.<sup>166</sup> A criminalization of the act in Phase 1 can address the divergent national attitudes with regard to the delineation of the preparatory acts at the early stages of the conduct. The legal concept of preparation raises questions as to how each legislation defines, or will define, the crime and the preparatory steps associated with it.

#### *Phase 2*

During the second phase the offenders obtain the identity-related information. As pointed out above,<sup>167</sup> there are various ways by which the offender can get possession over the information.

#### *Phase 3*

To include the third phase is a response to the fact that the identity-related information is not necessarily used by the offenders that obtained the information, but first of all transferred from one organized crime group to another.<sup>168</sup>

#### *Phase 4*

During the last phase the offenders use the identity-related information to commit offences or hide their identity.

<sup>165</sup> The model was developed by the author of the study in the context of a study on Internet-related Identity Theft for the Council of Europe in 2007. See Gercke, *Internet-related Identity Theft—A Discussion Paper*, Council of Europe, 2007.

<sup>166</sup> This is especially relevant in Phishing Cases. Regarding the different phases of phishing, see OECD Scoping Paper on Online Identity Theft, supra n. 13, page 18.

<sup>167</sup> See supra, chapter 4.3.

<sup>168</sup> Chawki/Abdel Wahab, *Identity Theft in Cyberspace: Issues and Solutions*, page 17, *Lex Electronica*, vol. 11, No. 1, 2006, available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited October 2008); OECD Scoping Paper on Online Identity Theft, supra n. 13, page 15.

### 3. Relation to identity-related information, but no unifying act

One of the few additional criteria the identity-related offences have in common is the fact that there is an interaction with identity-related information. The great diversity in the ways the acts are committed makes it difficult to find a head-category that summarizes the different acts. Neither “identity theft” nor “identity fraud” are useful in this context. One of the main concerns<sup>169</sup> related to the use of the term “identity theft” is the fact that in most cases the offenders do not remove the tangible item (which is an essential requirement of most theft provisions on a national level).<sup>170, 171</sup> Apart from dogmatic concerns, the term “theft” is not precise because in theft cases the person whose property is removed is in general the only victim, while in identity theft cases the person whose identity-related information is abused is not necessarily the only victim.<sup>172</sup> The term “identity fraud” is not precise because the motivation of the offenders who obtain identity-related information is not necessarily related to fraud. Despite the fact that a common term can be useful, it is therefore recommended to differentiate more precisely between identity-related crimes when discussing legal solutions.<sup>173</sup>

<sup>169</sup> Regarding those concerns, see *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, supra n. 141, page 553; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, 2008, page 8.

<sup>170</sup> Regarding the different dogmatic approach in the Roman law, see *Epstein/Brown*, Cybersecurity in the Payment Card Industry, *University of Chicago Law Review*, vol. 75, 2008, page 204.

<sup>171</sup> See *Ceaton*, The Cultural Phenomenon of Identity Theft..., supra n. 8, page 13, with further reference.

<sup>172</sup> Regarding the determination of the victim, see Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, page 11; Identity Theft, Available Data Indicate Growth in Prevalence and Cost, Statement of *R. Siana*, GAO Document: GAO-02-424T, 2002, page 5; *Levi/Burrows*, Measuring the Impact of Fraud in the United Kingdom, supra n. 22, page 12; *Elston/Stein*, International Cooperation in Online Identity Theft Investigations..., supra n. 10, page 5.

<sup>173</sup> *Levi/Burrows*, Measuring the Impact of Fraud in the United Kingdom, supra n. 22.





## VI. LEGAL APPROACHES

The criminalization of identity-related offences is one possible component of a response to the phenomenon.<sup>174</sup> The following chapter will provide an overview of the discussion dealing with the importance of a criminalization, national and international approaches and identity those criteria that play a key role in the development of a criminal law provision addressing identity-related offences.

### 1. Arguments in favour of and against a specific identity theft offence

While various countries have the possibility to prosecute certain aspects of identity theft related offences based on traditional provision such as fraud or forgery, only a few countries have implemented specific provisions criminalizing identity theft as a separate offence.<sup>175</sup> This indicates that the necessity of such solutions is not recognized globally. A similar situation can be observed with regard to the academic discussion. The main reason why states decide to criminalize identity theft is the recognition that primary abuse of identity can lead to a range of secondary crimes, thus enabling the criminal justice system to intervene at an earlier stage.<sup>176</sup>

### 2. General concerns regarding the criminalization of identity theft

Some experts have expressed fundamental concerns related to the criminalization of identity theft.<sup>177</sup> Ceaton points out that identity theft legislation does not solve the problem related to the phenomenon but “lays the foundation for the cultural phenomenon of identity theft—or what I have elsewhere called the myth of identity theft—which itself acts as

<sup>174</sup> For an overview about other approaches to prevent and combat Identity Theft, see supra chapter 1, as well as OECD Policy Guidance on Online Identity Theft, 2008.

<sup>175</sup> For an overview about identity theft legislation in Europe, see *Owen/Keats/Gill*, The Fight Against Identity Fraud: supra n. 159; *Mitchison/Wilikens/Breitenbach/Urry/Portesi*, Identity Theft—A Discussion Paper, supra n. 138, page 23 et seq.; *Legislative Approaches To Identity Theft...*, supra n. 159; For an overview about the legislation in Australia, the United States and the United Kingdom, see Discussion Paper Identity Crime, Model Criminal Law Officers’ supra n. 31; on the criminalization in the OECD Member States, see OECD Scoping Paper on Online Identity Theft, supra n. 13.

<sup>176</sup> Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, supra n. 10, page 3.

<sup>177</sup> See *Ceaton*, The Cultural Phenomenon of Identity Theft..., supra n. 8, page 13 et seq.

a robust instrument for both rationalizing the Web and operationalizing identity. [...] So citizens who might otherwise question the wisdom of reducing identity to quantifiable information, which then is concentrated in the hands of a few massive bureaucracies, are instead preoccupied with shredding their paper waste before disposing of it.”

The fundamental criticism is limited to criminal law, however, it targets legal solutions in general. Ceaton is in line with most experts in his intention to highlight that legal solutions cannot be the sole basis for a strategy aiming to reduce identity theft. As described above,<sup>178</sup> there are various issues that need to be taken into consideration within the drafting of such strategy. But this does not necessarily exclude legal measures.<sup>179</sup> If measures to prevent a behaviour that is going along with damages to a member of the society or a State itself is intended, the implementation of criminal law provisions can be legitimate and even necessary decision.

### 3. Applicability of traditional criminal law provisions

Identity theft is in general never a stand alone crime.<sup>180</sup> As highlighted above, the term identity theft is used to describe the combination of different acts.<sup>181</sup> They range from the theft of identity documents to the fraudulent use of identity-related information. Through analysis of so-called “identity theft” cases, it often turns out that traditional crimes like credit card fraud are only called “identity theft”.<sup>182</sup> The criminalization of theft and fraud has a long tradition in most countries. As based on the above-mentioned studies, the majority of identity-related offences are committed with the intention to commit fraud, in which case those acts can generally be prosecuted on the basis of the traditions criminal law provisions.

Even with regard to Internet-related identity theft cases, an introduction of a specific term is not necessarily required to be able to prosecute offences.<sup>183</sup> During the last ten years, many countries have updated their legislation to criminalize computer-related offences such as computer-related fraud and illegal access to computer systems. With regard to the fact that many cybercrime offences have a transnational dimension<sup>184</sup> and that differing legal standards in the countries involved can complicate the investigations,<sup>185</sup> a number of international organizations have picked up the topic with the aim to globally harmonize the national legislation and develop means of international cooperation.<sup>186</sup> One important approach is the Council of Europe Convention on Cybercrime, signed as of October 2008

<sup>178</sup> See supra, chapter 1.

<sup>179</sup> *Van der Meulen*, The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom and the European Union, Report commissioned by the National Infrastructure Cybercrime Programme (NICC), pages 25-26; FIDIS, deliverable 5.3: A Multidisciplinary Article on Identity-related Crime, pages 25-26; FIDIS, deliverable 5.2b: ID-related Crime: Towards a Common Ground for Interdisciplinary Research, pages 116-117.

<sup>180</sup> Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, supra n. 20, page 2.

<sup>181</sup> See supra, chapter 4.

<sup>182</sup> *Levi*, Combating Identity and Other Forms of Payment Fraud in the United Kingdom..., supra n. 55.

<sup>183</sup> *Gercke*, Internet-related Identity Theft, supra n. 165.

<sup>184</sup> Regarding the extend of transnational attacks in the most damaging cyber attacks, see *Sofaer/Goodman*, Cyber Crime and Security, supra n. 11, page 7.

<sup>185</sup> The background of those difficulties is often a requirement of dual criminality. Regarding the dual criminality principle see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, *Brigham Young University Law Review*, 1992, page 191 et seq., available at: <http://lawreview.byu.edu/archives/1992/1/haf.pdf> (last visited October 2008).

<sup>186</sup> For an overview on recent trends, see *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRI 2008, page 7 et seq.

by 45 States<sup>187</sup> and even more used to harmonize their laws without a formal signature.<sup>188</sup> The Convention on Cybercrime contains a number of substantive criminal law provisions that criminalize acts that are on a regular basis a part of Internet-related identity theft scams such as illegal access (Article 2) and the misuse of devices (Article 6).<sup>189</sup>

However, despite the general applicability of traditional substantive criminal law provisions, certain acts carried out within identity-related offences are not covered by the traditional substantive criminal law provisions and international instruments like the Convention on Cybercrime. One example is the transfer and sale of identity-related information.<sup>190</sup> While obtaining identity-related information and its use in fraudulent activities might be criminalized as theft and fraud, the exchange and trade of such information is neither widely recognized as a criminal offence nor to a full extent covered by the Convention on Cybercrime. The development of a specific criminal law provision can close those possible gaps in the national legislation.

#### 4. Precise definition of the object of legal protection

As described earlier, identity-related information plays a crucial role in social life. Most of those traditional criminal law provisions that can be used to prosecute single aspects of identity-related offences, such as fraud and forgery, are not designed to protect identity-related information but instead, other fundamental values such as confidence of the marked in the reliability of documents. A specific approach to criminalize identity theft enables the lawmaker to respond to the growing importance of identity-related information by creating a criminal law provision that focuses on this information as the object of legal protection.

#### 5. Practical aspects related to the investigation

As pointed out above, identity theft is in general never a stand alone crime.<sup>191</sup> The criminalization of identity theft would enable law enforcement agencies to prosecute the chronologically earlier act. Such an ability could avoid difficulties in the identification of the offender committing the subsequent acts.<sup>192</sup>

<sup>187</sup> The current list of signatures and ratifications is available on the Council of Europe website: <http://www.coe.int>.

<sup>188</sup> Regarding the Convention, see *Sofaer*, *Toward an International Convention on Cyber Security in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror*, page 225, available online: [http://media.hoover.org/documents/0817999825\\_221.pdf](http://media.hoover.org/documents/0817999825_221.pdf) (last visited October 2008); *Gercke*, *The Slow Awake of a Global Approach Against Cybercrime*, *CRi*, 2006, page 140 et seq.; *Gercke*, *National, Regional and International Approaches in the Fight Against Cybercrime*, supra n. 186, page 7 et seq.; *Aldesco*, *The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime*, *Entertainment Law Review*, 2002, No. 1, available at: <http://elr.ils.edu/issues/v23-issue1/aldesco.pdf> (last visited October 2008); *Jones*, *The Council of Europe Convention on Cybercrime, Themes and Critiques*, 2005, available at: <http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf> (last visited October 2008); *Broadhurst*, *Development in the Global Law Enforcement of Cyber-Crime*, in *Policing: An International Journal of Police Strategies and Management*, vol. 29, No. 2, 2006, page 408 et seq.; *Adoption of Convention on Cybercrime*, *International Journal of International Law*, vol. 95, No. 4, 2001, page 889 et seq.

<sup>189</sup> For a more detailed analysis of the application of provisions mentioned in the Convention on Cybercrime with regard to identity-related offences, see *Gercke*, *Internet-related Identity Theft*, supra n. 165, page 23 et seq.

<sup>190</sup> *Ibid.*, page 27.

<sup>191</sup> *Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited*, supra n. 20, page 2.

<sup>192</sup> *Identity Fraud: A Study*, United Kingdom Cabinet Office, 2002, page 5, available at: <http://www.ips.gov.uk/identity/downloads/id-fraud-report.pdf> (last visited October 2008).

## 6. Conflict between national and international dimensions

Identity theft offences have very often a transnational dimension.<sup>193</sup> Given the involvement of organized crime groups, this trend towards a globalization of the offences is very likely to continue.<sup>194</sup> This transnational dimension raises concerns regarding national approaches to criminalize identity theft. The fact that differing national standards can hinder international investigations supports international approaches instead, or at least in addition to, national solutions. However, no such globally applicable legal instruments are currently available. As a result, the potential conflict between national and international solutions is rather theoretical at the moment.

## 7. International approaches

Currently, the development of legal frameworks to criminalize identity theft is only taking place on a national level.<sup>195</sup> Until today, none of the international organizations that deals with issues related to criminal law has developed a specific identity theft legislation containing criminalization provisions of the related acts. But despite the missing globally applicable criminal law standards, the international and regional organizations have increased their activities related to this issue.

### *United Nations*

The problems posed by identity-related crime have acquired a prominent place in the crime prevention and criminal justice agenda of the United Nations. The Bangkok Declaration on “Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice”,<sup>196</sup> endorsed by General Assembly resolution 60/177 of 16 December 2005, underlined the crucial importance of tackling document and identity fraud in order to curb organized crime and terrorism.<sup>197</sup> Member States were also called upon “to improve international cooperation, including through technical assistance, to combat document and identity fraud, in particular the fraudulent use of travel documents, through improved security measures, and encourage the adoption of appropriate national legislation”.<sup>198</sup>

<sup>193</sup> *Elston/Stein*, International Cooperation in Online Identity Theft Investigations..., supra n. 10.

<sup>194</sup> Regarding the organized crime dimension, see *McCusker*, Transnational Organized Cybercrime: Distinguishing Threat From Reality, *Crime, Law and Social Change*, vol. 46, page 273; *Choo/Smith*, Criminal Exploitation of Online Systems by Organized Crime Groups, *Asian Criminology*, 2008, page 37 et seq.; Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, supra n. 10, page 11.

<sup>195</sup> For an overview about identity theft legislation in Europe, see *Owen/Keats/Gill*, The Fight Against Identity Fraud..., supra n. 159; *Mitchison/Wilkens/Breitenbach/Urry/Portesi*, Identity Theft, supra n. 138; Legislative Approaches To Identity Theft: An Overview, supra n. 159; for an overview about the legislation in Australia, the United States and the United Kingdom see: Discussion Paper Identity Crime, Model Criminal Law Officers’ Committee, supra n. 31, 2007; Regarding the criminalization in the OECD member states, see OECD Scoping Paper on Online Identity Theft, supra n. 13.

<sup>196</sup> Bangkok Declaration, Synergies and Responses: Strategic Alliance in Crime Prevention and Criminal Justice”, 2005, endorsed by General Assembly resolution 60/177 of 16 December 2005, available at: <http://www.un.org/events/11thcongress/declaration.htm> (last visited October 2008).

<sup>197</sup> Regarding the links between identity-related crimes and organized crime and terrorism, see Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, supra n. 10, page 11.

<sup>198</sup> Bangkok Declaration, Synergies and Responses: Strategic Alliance in Crime Prevention and Criminal Justice, 2005, paragraph 27.



Pursuant to Economic and Social Council (ECOSOC) resolution 2004/26, UNODC commissioned a study on “fraud and the criminal misuse and falsification of identity” which was released in early 2007.<sup>199</sup> The study’s approach was broader than that followed in the OECD context: first, the general term “identity-related crime” has been used to cover all forms of illicit conduct involving identity, including offences described, often not in a consistent manner, as “identity fraud” and “identity theft”; second, criminal acts related to identity theft were considered in their entirety to include their commission both online and offline, with more emphasis on sophisticated criminal schemes and patterns due to existing linkages to transnational organized crime and other criminal activities; and, third, identity-related crime was considered jointly with fraud given their close relationship and the specific directions of the ECOSOC mandate.

The Report of the Secretary-General of the United Nations on Recommendations for a Global Counter-Terrorism Strategy highlights the importance of developing tools to tackle identity theft in the fight against terrorism.<sup>200</sup> In addition, the challenges related to identity theft as well as the need for an adequate response are mentioned in different United Nations resolutions. An example is the Resolution on Strengthening the United Nations Crime Prevention<sup>201</sup> which highlights identity theft as one of the emerging policy issues that should be explored by UNODC. Based on ECOSOC Resolution 2004/26<sup>202</sup> and ECOSOC Resolution 2007/20,<sup>203</sup> UNODC has established a group of experts to exchange views on the best course of action in this field.<sup>204</sup>

## OECD

In 1999, the OECD Council approved a set of guidelines designed to protect the electronic commerce.<sup>205</sup> The measures in these guidelines can be used to develop strategies to prevent identity-theft. Due to the soft-law character of the guidelines they do not contain approaches to criminalize specific aspects of identity theft. In 2003, the OECD developed another guideline on aspects of cross-border fraud.<sup>206</sup> Similarly to the 1999 Guidelines, they do not explicitly deal with an approach on how to criminalize identity theft but can be used to develop the broader framework necessary to effectively investigate and prosecute those offences. In 2008 the OECD published a “Scoping Paper on Online Identity Theft”<sup>207</sup> that in addition to providing a detailed analysis of different Internet-related identity theft scams,

<sup>199</sup> The report containing the results and findings of the study on “fraud and the criminal misuse and falsification of identity” was submitted to the Commission on Crime Prevention and Criminal Justice at its sixteenth session (E/CN.15/2007/8 and Add. 1-3).

<sup>200</sup> Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy, 27.04.2006, A/60/825, page 13.

<sup>201</sup> United Nations General Assembly Resolution, Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity, A/RES/62/175, 2008, page 3.

<sup>202</sup> ECOSOC Resolution 2004/26 on “International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes”.

<sup>203</sup> ECOSOC Resolution 2007/20 on “International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime”.

<sup>204</sup> Reports related to the activities of the core group are available in the public domain. See First meeting of the Core Group of Experts on Identity-Related Crime Cormier Mont Blanc, Italy, 29-30 November 2007, available at: [http://www.unodc.org/documents/organized-crime/Courmayeur\\_report.pdf](http://www.unodc.org/documents/organized-crime/Courmayeur_report.pdf) (last visited October 2008); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, available at: [http://www.unodc.org/documents/organized-crime/Final\\_Report\\_ID\\_C.pdf](http://www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf) (last visited October 2008).

<sup>205</sup> OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, available at: <http://www.oecd.org/dataoecd/18/13/34023235.pdf> (last visited October 2008).

<sup>206</sup> OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, available at: [http://www.oecd.org/document/56/0,3343,en\\_2649\\_34267\\_2515000\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/56/0,3343,en_2649_34267_2515000_1_1_1_1,00.html).

<sup>207</sup> Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL.

deals with aspects related to the victims as well as law enforcement schemes. Also in 2008, the OECD published the “Policy Guidance on Online Identity Theft.”<sup>208</sup> This guidance provides an overview about different strategies to respond to Internet-related identity theft.

### *European Union*

The European Union has developed different legal instruments that deal with identity-related information such as the EU Directive on the Privacy,<sup>209</sup> as well as the criminalization of certain aspects of fraud<sup>210</sup> and Internet-related offences such as illegal access to computer systems.<sup>211</sup> Yet none of the measures contain criminal law provisions that specifically address identity theft.

However, the challenges posed by related criminal activities have already been recognized at the European Union level as a considerable policy issue,<sup>212</sup> while the European Commission has further proposed that “EU law enforcement cooperation would be better served were identity theft criminalized in all Member States”.<sup>213</sup> This proposal paved the ground for conducting consultations to assess whether specific legislation is necessary and appropriate in member states, as it is reasonable to suggest that there will be increasing public attention in Europe to preventing and responding efficiently to identity abuses for criminal purposes. The Commission (DG on Justice, Freedom and Security) has already launched a comparative study in July 2007 on the definitions of identity theft used in the EU Member States and their criminal consequences.<sup>214</sup>

### *Council of Europe*

In 2001 the Council of Europe Convention on Cybercrime was opened for signature.<sup>215</sup> During the ceremony itself, 30 countries signed the Convention (including the four non-members of the Council of Europe Canada, United States, Japan and South Africa that

<sup>208</sup> OECD Policy Guidance on Online Identity Theft, 2008.

<sup>209</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>210</sup> EU Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, 2001/413/JHA.

<sup>211</sup> Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems; for more information, see *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, page 468 et seq.

<sup>212</sup> As part of an awareness campaign to improve the prevention of identity theft and payment fraud, Directorate-General Justice, Freedom and Security (DG JLS) and Directorate-General Internal Market of the European Commission organized a conference on “Maintaining the integrity of identities and payments: Two challenges for fraud prevention”, which took place on 22–23 November 2006 in Brussels. The Conference intended to emphasize the importance of the wider involvement of policy makers and high ranking representatives of national administrations and to provide a platform for policy makers to discuss possible EU initiatives in this field. Among the issues discussed at the Conference were possible EU criminal legislation on identity theft, training models for law enforcement/financial investigators, exchange of information and privacy issues.

<sup>213</sup> European Commission, Communication from the Commission to the European Parliament, the Council and the Committee of the Regions—Towards a general policy on the fight against cybercrime, COM (2007)267, 22 May 2007.

<sup>214</sup> This study will include, upon its finalization, recommendations on best practices.

<sup>215</sup> Regarding the Convention, see *Sofaer*, Toward an International Convention on Cyber Security, supra n. 188, page 225; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, *ibid.*, page 140 et seq.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, supra n. 186, page 7 et seq.; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, supra n. 188; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: <http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf> (last visited October 2008); *Broadhurst*, Development in the Global Law Enforcement Of Cyber-Crime, supra n. 188, page 408 et seq.; Adoption of Convention on Cybercrime, *ibid.*, page 889 et seq.

participated in the negotiations). By October 2008, 45 States<sup>216</sup> had signed and 23 States<sup>217</sup> had ratified<sup>218</sup> the instrument. The Convention, which contains substantive criminal law provisions criminalizing acts like illegal access to computer systems or system interference, is today recognized as an important international instrument in the fight against cybercrime and is supported by different international organizations.<sup>219</sup>

In 2007, the Council of Europe published a study which analyzed the different approaches in criminalizing Internet-related identity theft. The study pointed out that despite the applicability of the provisions in the Convention on Cybercrime in identity theft cases, it did not contain a specific provision addressing identity theft per se which could be applicable with regard to all related acts.<sup>220</sup>

## 8. National approaches

As mentioned above, some countries have already implemented provisions that go beyond the traditional approaches to criminalize forgery or fraud but explicitly focus on identity theft related acts.

### *United States*

In 1998, the United States introduced a specific criminalization of acts related to identity theft with 18 U.S.C. § 1028(a)(7).<sup>221</sup> The provision covers a wide range of offences related to identity theft. In 2004 penalties for aggravated identity theft was introduced. A draft Identity Theft Enforcement and Restitution Act that focuses on closing existing gaps in the legislation was presented in 2007 and was recently passed in the United States Senate, although it has not yet come into force:

<sup>216</sup> Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, the Former Yugoslav Republic of Macedonia, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Moldova, Romania, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Ukraine, the United Kingdom, the United States.

<sup>217</sup> Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, the Former Yugoslav Republic of Macedonia, France, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Slovakia, Slovenia, Ukraine, the United States.

<sup>218</sup> The need for a ratification is laid down in Article 36 of the Convention.

<sup>219</sup> Interpol highlighted the importance of the Convention on Cybercrime in the Resolution of the sixth International Conference on Cyber Crime, Cairo: “That the Convention on Cyber Crime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cybercrime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages.”, available at: <http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp> (last visited October 2008); The 2005 WSIS Tunis Agenda points out: “We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on “Combating the criminal misuse of information technologies” and regional initiatives including, but not limited to, the Council of Europe’s Convention on Cybercrime”, available at: [http://ec.europa.eu/information\\_society/activities/internationalrel/docs/wsisis/tunis\\_agenda.pdf](http://ec.europa.eu/information_society/activities/internationalrel/docs/wsisis/tunis_agenda.pdf) (last visited October 2008).

<sup>220</sup> Gercke, Internet-related Identity Theft, supra n. 165.

<sup>221</sup> Identity Theft and Assumption Deterrence Act 1998. For further information about the act, see Zaidi, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada, *Loyola Consumer Law Review*, vol. 19, issue 2, page 99 et seq.; Finkelstein, Memorandum for Assistant Regional Council on Identity Theft and Assumption Deterrence Act of 1998, 1999, available at: <http://www.unclefed.com/ForTaxProfs/irs-wd/1999/9911041.pdf>; Gordon/Wilcox/Rebovich/Regan/Gordon, Identity Fraud: A Critical National and Global Threat, *Journal of Economic Management*, 2004, vol. 2, issue 1.

*1028. Fraud and related activity in connection with identification documents, authentication features, and information*

(a) Whoever, in a circumstance described in subsection (c) of this section:

[...]

(7) Knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

[...]

shall be punished as provided in subsection (b) of this section.

*1028A. Aggravated identity theft*

(a) Offenses:

(1) In general. Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

As highlighted above, the provision is a broad approach to criminalize various forms of identity theft. By criminalizing the “transfer” of means of identification with the intent to commit an offence, the provision enables the prosecution of offences related to the above mentioned Phase 3 that is very often not covered by traditional approaches. Yet given that the provisions focus on the direct interaction with identity-related data, preparatory acts like sending out phishing mails and designing malicious software that can be used to obtain computer identity-related data from the victims are not covered by 18 U.S.C. § 1028(a)(7) and 18 U.S.C. 1028A(a)(1). The Identity Theft Enforcement and Restitution Act of 2007 is undertaking an approach to close those gaps, for example by criminalizing certain acts related to spyware and keyloggers.

## Canada

In 2007 Canada introduced a draft law to create a specific identity theft related criminal offence.<sup>222</sup> The draft law contains two relevant provisions: 402.1 defines the covered identity-related information while 402.2 contains the criminalized acts.

### 402.1

For the purposes of sections 402.2 and 403, “identity information” means any information—including biological or physiological information—of a type that is

<sup>222</sup> See: <http://www.parl.gc.ca/LEGISINFO/index.asp?List=ls&Query=5333&Session=15&Language=e#idtheft> (last visited October 2008). In October 2009, Bill S-4 was adopted as an amendment to the Canadian Criminal Code (identity theft and related misconduct).

commonly used alone or in combination with other information to identify or purport to identify an individual, such as a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's license number or password.

#### 402.2

- 1) Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.
- 2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for any of those purposes, knowing or believing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.
- 3) For the purposes of subsections (1) and (2), an indictable offence referred to in either of those subsections includes an offence under any of the following sections:
  - (a) section 57 (forgery of or uttering forged passport);
  - (b) section 58 (fraudulent use of certificate of citizenship);
  - (c) section 130 (personating peace officer);
  - (d) section 131 (perjury);
  - (e) section 342 (theft, forgery, etc., of credit card);
  - (f) section 362 (false pretence or false statement);
  - (g) section 366 (forgery);
  - (h) section 368 (uttering, trafficking or possessing with intent forged document);
  - (i) section 380 (fraud); and
  - (j) section 403 (identity fraud).

The draft legislation contains a number of interesting approaches. It first of all provides examples for the identity information which is covered by the provision, without narrowing the application of the provision.<sup>223</sup> In addition it provides a set of indictable offences. While this, on the one hand, narrows the applicability, it is, on the other, a very precise approach. Finally, it covers a wide range of offences. Similarly to the United States approach, the Canadian draft law does not cover preparatory acts as sending out phishing e-mails or designing malicious software.<sup>224</sup>

<sup>223</sup> The term "such as" used in the 402.1 leaves space for an open interpretation if necessary, for example due to technical developments.

<sup>224</sup> This does not necessarily mean that such acts are not criminalized by different provisions.

## 9. Essential elements of a legal approach

Developing a legal response to identity theft that goes beyond the adjustment of traditional instruments by creating specific provision requires a number of decisions and adjustments. An overview about those essential elements is provided below.

### *Identity*

It is necessary to define the protected identity-related information. If an offender illegally enters a computer to obtain business secrets, this offence targets digital information but due to the missing link to identity-related information it would not be considered an identity-related offence. Within the definition there are several aspects that need to be taken into consideration:

#### *Scope of definition*

It is necessary to decide if a broad or a more precise definition of the identity-related information should be implemented.<sup>225</sup> The answer to the question depends on the underlying legal system as well as the legal tradition, in addition to the regional importance of certain identity-related data.<sup>226</sup> While a closed enumeration is in general more precise, it carries the risks of difficulties in the application after fundamental technical changes.

Some digital data, such as passwords, account names and login information, may not be considered elements of a person's legal identity. But taking into account the use of data to log on to digital services,<sup>227</sup> it is necessary to decide if that information needs to be included in the definition.<sup>228</sup>

#### *Synthetic identities*

In addition, it is necessary to decide if only acts related to real identities should be covered, or if even the use of fictitious identity-related information should be criminalized.<sup>229</sup> As pointed out above, the criminalization of the use of fictitious identities does not, at first sight, seem to be relevant, as in those cases where there is no impact for a legitimate user of an identity. Still, the absence of a natural person who is affected by the offence does not mean that such acts do not cause damage. By using synthetic identities offenders can mislead investigations and make his identification more difficult.<sup>230</sup> A major part of fraud-related cases are not based on true-name identities but

<sup>225</sup> In favour of a broad approach: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee supra n. 31, page 25.

<sup>226</sup> One example is the Social Security Number, which is of great relevance in the United States but not, for example, in Europe. Regarding the SSN, see *Sobel*, The Demeaning of Identity and Personhood in National Identification Systems, *Harvard Journal of Law & Technology*, vol. 15, No. 2, 2002, page 350.

<sup>227</sup> See supra, chapter 3.2.4.

<sup>228</sup> *Paget*, Identity Theft, McAfee White Paper, page 4, 2007, available at: [http://www.mcafee.com/us/threat\\_center/white\\_paper.html](http://www.mcafee.com/us/threat_center/white_paper.html) (last visited October 2008).

<sup>229</sup> For an overview of the arguments in favour of including synthetic Identities, see Discussion Paper Identity Crime, Model Criminal Law Officers' Committee, supra n. 31, page 25.

<sup>230</sup> Regarding synthetic identities related identity theft scams, see *Schneier*, Synthetic Identity Theft, 05.11.2007, available at: [http://www.schneier.com/blog/archives/2007/11/synthetic\\_ident.html](http://www.schneier.com/blog/archives/2007/11/synthetic_ident.html) (last visited October 2008); *McFadden*, Detecting Synthetic Identity Fraud, available at: [http://www.bankrate.com/brm/news/pf/identity\\_theft\\_20070516\\_a1.asp](http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp) (last visited October 2008).

synthetic identities.<sup>231</sup> Based on the results of a study by ID Analytics, less than 15 per cent of all cases involved true-name identities.<sup>232</sup> Synthetic identities can either be based solely on generated data or combine generated and real identity-related data.<sup>233</sup> Within the drafting process it is therefore necessary to decide if an interference with an existing identity is a necessary requirement for the criminalization.

### *Covered acts/phases*

In a second step, it is necessary to determine the acts that should be criminalized by the offence. A distinction between the four different phases that have been developed above can help to prevent gaps as well as an overlapping:

#### *Phase 1 (Preparatory acts)*

All non-spontaneous offences in general include a preparation phase that is usually not necessarily criminalized. With regard to identity-related offences, a decision is necessary if preparatory acts like designing malicious software to obtain identity-related information or sending out phishing e-mails shall already be criminalized. The fact that the drafters of the Convention on Cybercrime included a provision which criminalizes the development of software tools to commit certain computer-related offences, such as illegally entering a computer system, demonstrates that there is a tendency towards a criminalization of preparatory acts. But those approaches draw concerns related to over-criminalization. Especially in those cases where the national criminal law system does not widely criminalize the preparation of crimes, acts related to phase 1 could be excluded from the criminalization.

#### *Phase 2 (Obtaining the information)*

Obtaining identity-related information is a widely accepted aspect of identity theft. The offenders use different methods to obtain identity-related information. Both national approaches that were presented above cover the diverse methods by criminalizing the “obtaining”/”transfer” of identity-related information.

In this context, two specific scenarios need to be taken into consideration. First, a number of identity theft related scams are based on the disclosure of identity-related information by the victim as a result of use of social engineering techniques. In those cases, it is likely that provisions incorporating the act of “obtaining” could more easily be applied compared to provisions that require a “transfer” of identity-related information by the offender. A second scenario, where similar difficulties could appear, is the collection of publicly available identity-related information.

<sup>231</sup> See ID Analytics, [http://www.idanalytics.com/assets/pdf/National\\_Fraud\\_Ring\\_Analysis\\_Overview.pdf](http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf) (last visited October 2008).

<sup>232</sup> Ibid.

<sup>233</sup> See 2007 Identity Fraud Survey Report, Consumer Version, Javelin Strategy and Research, 2007, page 10, available at: [http://www.acxiom.com/AppFiles/Download18/Javelin\\_ID\\_Theft\\_Consumer\\_Report-627200734724.pdf](http://www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf) (last visited October 2008).

### *Phase 3 (Transfer process)*

The third phase is characterized by a transfer of identity-related information.<sup>234</sup> Those approaches that include acts like “transferring” or even more concrete “transmitting” or “selling” are generally applicable in those cases. For those countries that have not implemented specific identity theft related offences and therefore need to apply traditional substantive criminal law provisions like fraud and forgery, the prosecution of acts related to this category brings the most difficulties compared to the other categories.

### *Phase 4 (Use for criminal purposes)*

As diverse as the methods used to obtain identity-related information are the motivations of the offenders and the way they act by using the identity-related information. In general there are two different approaches related to the criminalization of acts in this fourth phase. With regard to the fact that the most common ways in which the identity-related information is used (for example to commit fraud) are already covered by traditional substantive criminal law provisions, some approaches do not include acts related to the fourth phase but only include a link to those offences by requiring an intent to commit one of the offences.<sup>235</sup> Other approaches criminalize the use of the identity-related information (with the intent to commit an illegal activity) in addition to the intended offence itself.

## *Without authorization/illegally*

It is necessary to decide if the criminalization requires that the offender acted without the permission of the person whose identity-related information is concerned. In general, the exclusion of authorized and legitimate acts is necessary to ensure that the criminalization of identity theft does not negatively influence the ability of businesses to exchange identity-related information where necessary.<sup>236</sup> Yet as pointed out above, excluding those acts where information which is used was voluntarily disclosed could exclude acts like phishing or the use of information gathered from public sources.

## *Dishonesty*

One of the essential requirements of the criminalization of identity theft is to avoid an interference with legitimate operations. One approach discussed to avoid such interference is to require dishonesty as an additional element for criminalization purposes.<sup>237</sup> Despite the advantages of avoiding an unintended criminalization, the proof of such dishonesty can bring challenges.

<sup>234</sup> Regarding the importance of criminalizing this phase of the offence, see Discussion Paper Identity Crime, Model Criminal Law Officers’ Committee, supra n. 31, page 25.

<sup>235</sup> Regarding the intent to commit further crimes, see infra: chapter 6.9.7.

<sup>236</sup> This can, for example, be necessary for the billing of credit cards.

<sup>237</sup> Discussion Paper Identity Crime, Model Criminal Law Officers’ Committee, supra n. 31, page 27.



### *Intent to commit another offence*

Identity theft is in general not a stand-alone crime. To avoid an over-criminalization, the offence could be limited to acts that are linked to further offences. Both the United States approach as well as the Canadian draft law contains such a link. While the United States legislation requires that the offender acted with the intent to commit any unlawful activity, the Canadian draft law only requires that circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence. With regard to the transfer of identity-related information, the Canadian draft law goes beyond this by criminalizing offenders who were reckless as to whether the information will be used to commit an indictable offence.

### *Mental element*

Finally, a decision about the regular mental element (in allocation of the special intent mentioned above) needs to be taken. Both the United States approach and the Canadian draft law require that the offender acted with knowledge.



# REFERENCES

## Publications

1. *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cyber-crime, *Entertainment Law Review*, 2002, No. 1, available at: <http://elr.ils.edu/issues/v23-issue1/aldesco.pdf> (last visited October 2008).
2. *Biegel*, Beyond our Control? Confronting the Limits of our Legal System in the Age of Cyberspace, Massachusetts Institute of Technology, 2001.
3. *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, *Chicago Journal of International Law*, 2007, vol. 8, No. 1, available at: [http://eprints.law.duke.edu/archive/00001602/01/8\\_Chi.\\_J.\\_Int'l\\_L.\\_233\\_\(2007\).pdf](http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf) (last visited October 2008).
4. *Bolton/Hand*, Statistical Fraud Detection: A Review, 2002, available at: <http://metalab.uniten.edu.my/~abdrahim/ntl/Statistical%20Fraud%20Detection%20A%20Review.pdf> (last visited October 2008).
5. *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, *European Law Journal*, 2005.
6. *Broadhurst*, Development in the global law enforcement of cyber-crime, in *Policing: An International Journal of Police Strategies and Management*, vol. 29, No. 2, 2006.
7. *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, *Lex Electronica*, vol. 11, No. 1, 2006, available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited October 2008).
8. *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, *Bulletin of Science Technology Society*, 2007, vol. 27, 2008.
9. *Clarke*, Technology, Criminology and Crime Science, *European Journal on Criminal Policy and Research*, vol. 10, 2004.
10. *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, Kluwer Academic Publishers, 1999.
11. *Copes/Vieraitis/Jochum*, Bridging the Gap between Research and Practice: How Neutralization Theory Can Inform Reid Interrogations of Identity Thieves, *Journal of Criminal Justice Education*, vol. 18, No. 3, 2007.
12. *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: [http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf) (last visited October 2008).
13. *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, O'Reilly, 2006.
14. *Elston/Stein*, International Cooperation in Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf> (last visited October 2008).

15. *Emigh*, Online Identity Theft: Phishing Technologies, Chokeypoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005.
16. *Epstein/Brown*, Cybersecurity in the Payment Card Industry, *University of Chicago Law Review*, vol. 75, 2008.
17. *Faulkner*, Hacking Into Data Breach Notification Laws, *Florida Law Review*, vol. 59, 2007.
18. *Fawcett/Provost*, Adaptive Fraud Detection, *Data Mining and Knowledge Discovery*, vol. 1, No. 3, 1997.
19. *Garfinkel*, Database nation: The Death of Privacy in the 21st Century, O'Reilly, 2000.
20. *Gayer*, Policing Privacy, Law Enforcement's Response to Identity Theft, CALPIRG Education Fund, 2003.
21. *Gercke*, Criminal Responsibility for Phishing and Identity Theft, *Computer und Recht*, 2005.
22. *Gercke*, The Challenge of Fighting Cybercrime, *Multimedia und Recht*, 2008.
23. *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, *CRi*, 2006.
24. *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, *CRi* 2008.
25. *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: [http://www.privacyrights.org/ar/id\\_theft.htm](http://www.privacyrights.org/ar/id_theft.htm) (last visited October 2008).
26. *Gonsalves*, Phishers Snare Victims with VoIP, 2006, available at: <http://www.techweb.com/wire/security/186701001> (last visited October 2008).
27. *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003.
28. *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, *Security Focus*, 2001, available at: <http://www.securityfocus.com/infocus/1527> (last visited October 2008).
29. *Gross/Acquisti*, Information Revelation and Privacy in Online Social Networks, 2005, available at: <http://wiki.cs.columbia.edu:8080/download/attachments/1979/Information+Revelation+and+Privacy+in+Online+Social+Networks-gross.pdf> (last visited October 2008).
30. *Guo/Chiueh*, Sequence Number-Based MAC Address Spoof Detection, available at: <http://www.ecsl.cs.sunysb.edu/tr/TR182.pdf> (last visited October 2008).
31. *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, *Brigham Young University Law Review*, 1992, available at: <http://lawreview.byu.edu/archives/1992/1/haf.pdf> (last visited October 2008).
32. *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, *CJI* 2002, vol. 18, available at: <http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37> (last visited October 2008).
33. *Halperin*, Identity as an Emerging Field of Study, *Datenschutz und Datensicherheit*, 2006.
34. *Hansen/Meissner* (ed.), Linking digital identities, 2007, available at: <https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf> (last visited October 2008).
35. *Hoar*, Identity Theft: The Crime of the New Millennium, *Oregon Law Review*, vol. 80, 2001.
36. *Hayden*, Cybercrime's impact on Information security, *Cybercrime and Security*, IA-3.
37. *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, *Computer und Recht International*, 2006.
38. *Jagatic/Johnson/Jakobsson/Menczer*, Social Phishing, 2005, available at: <http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf> (last visited October 2008).

39. *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, *EJIL* 2002, No. 5.
40. *Kang*, Wireless Network Security—Yet another hurdle in fighting Cybercrime in *Cybercrime & Security*, IIA-2.
41. *Keyser*, The Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, vol. 12, No. 2, available at: [http://www.law.fsu.edu/journals/transnational/vol12\\_2/keyser.pdf](http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf) (last visited October 2008).
42. *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, *Datenschutz und Datensicherheit*, 2006.
43. *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, 2008.
44. *Levi*, Combating Identity and Other Forms of Payment Fraud in the United Kingdom: An Analytical History, published in *McNally/Newman*, Perspectives on Identity Theft.
45. *Levi/Burrows*, Measuring the Impact of Fraud in the United Kingdom, *British Journal of Criminology*, vol. 48, 2008.
46. *Lewis*, Cyber Attacks Explained, 2007, available at: [http://www.csis.org/media/csis/pubs/070615\\_cyber\\_attacks.pdf](http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf) (last visited October 2008).
47. *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005.
48. *Mashima/Ahamad*, Towards a User-Centric Identity-Usage Monitoring System, in *Internet Monitoring and Protection*, 2008.
49. *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, *Crime, Law and Social Change*, vol. 46.
50. *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: <http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf> (last visited October 2008).
51. *Owen/Keats/Gill*, The Fight Against Identity Fraud: A Brief Study of the EU, the United Kingdom, France, Germany, and the Netherlands, Perpetuity Research & Consultancy International, 2006.
52. *Paget*, Identity Theft, McAfee White Paper, 2007, available at: [http://www.mcafee.com/us/threat\\_center/white\\_paper.html](http://www.mcafee.com/us/threat_center/white_paper.html) (last visited October 2008).
53. *Putnam/Elliott*, “International Responses to Cyber Crime”, in *Sofaer/Goodman*, “Transnational Dimension of Cyber Crime and Terrorism”, 2001.
54. *Romanosky/Relang/Acquisti*, Do Data Breach Disclosure Laws Reduce Identity Theft?, Seventh Workshop on the Economics of Information Security, Center for Digital Strategies, Tuck School of Business, available at: <http://weis2008.econinfosec.org/papers/Romanosky.pdf> (last visited October 2008).
55. *Roth*, “State Sovereignty, International Legality, and Moral Disagreement”, 2005, available at: <http://www.law.uga.edu/intl/roth.pdf> (last visited October 2008).
56. *Siegel*, Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age, *Penn State Law Review*, vol. 111, No. 3.
57. *Sobel*, The Demeaning of Identity and Personhood in National Identification Systems, *Harvard Journal of Law & Technology*, vol. 15, No. 2, 2002.
58. *Sofaer/Goodman*, Cyber Crime and Security—The Transnational Dimension, in *Sofaer/Goodman*, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001, page 1 et seq.,

available at: [http://media.hoover.org/documents/0817999825\\_1.pdf](http://media.hoover.org/documents/0817999825_1.pdf) (last visited October 2008).

59. *Shamah*, Password Theft: Rethinking an old crime in a new area, *Mich. Telecomm. Tech. Law Review*, vol. 12, 2006.
60. *Stevens*, Federal Information Security and Data Breach Notification Laws, 3 April 2008, CRS Report for Congress, Document RL34120.
61. *Stoddart*, Who Watches the Watchers? Towards an Ethic or Surveillance in a Digital Age, *Studies in Christian Ethics*, 2008, vol. 21, 2008.
62. *Stutzman*, An Evaluation of Identity-Sharing Behavior in Social Network Communities, available at: [http://www.ibiblio.org/fred/pubs/stutzman\\_pub4.pdf](http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf) (last visited October 2008).
63. *Sury*, Identity-Management und Recht, *Informatik-Spektrum*, vol. 27, No. 3, 2004.
64. *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, Routledge 2001.
65. *Turner*, Towards a Rational Personal Data Breach Notification Regime, Information Policy Institute, June 2006.
66. *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: <http://www.aic.gov.au/publications/tandi2/tandi329t.html> (last visited October 2008).
67. *Van der Meulen*, The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom and the European Union, Report commissioned by the National Infrastructure Cybercrime Programme (NICC).
68. *Wang/Chen/Atabakhsh*, Criminal Identity Deception and Deception Detection in *Law Enforcement, Group Decision and Negotiation*, vol. 13, 2004.
69. *White/Fisher*, Assessing Our Knowledge of Identity Theft: The Challenge of Effective Prevention and Control Efforts, *Criminal Justice Policy Review*, 2008, vol. 19, 2008.
70. *Wright*, Detecting Wireless LAN Mac Address Spoofing, 2003, available at: <http://forskning-snett.uninett.no/wlan/download/wlan-mac-spoof.pdf> (last visited October 2008).
71. *Zaidi*, Identity Theft and Consumer Protection: Finding Sensible Approaches to Safeguard Personal Data in the United States and Canada, *Loyola Consumer Law Review*, vol. 19, issue 2, 2007.


## Studies/surveys/reports/discussion papers

72. 2003 Federal Trade Commission Identity Theft Survey Report.
73. 2006 Better Bureau Identity Fraud Survey.
74. 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data.
75. 2007 Javelin Strategy and Research Identity Fraud Survey.
76. Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007.
77. Identity Fraud: A Study, United Kingdom Cabinet Office, 2002, available at: <http://www.ips.gov.uk/identity/downloads/id-fraud-report.pdf> (last visited October 2008).
78. Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR.

79. Identity Theft—A Discussion Paper, available at: <https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf> (last visited October 2008).
80. Identity Theft, Available Data Indicate Growth in Prevalence and Cost, Statement of R. Stana, GAO Document: GAO-02-424T.
81. Identity Theft, Greater Awareness and Use of Existing Data Are Necessary, Report to the Honourable Sam Johnson, House of Representatives, GAO Document: GAO-02-766.
82. Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07-935T.
83. Internet-related Identity Theft, 2007, available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf](http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf) (last visited October 2008).
84. Lessons Learned about Data Breach Notification, Report to Congressional Requesters, 2007, GAO Document: GAO-07-657.
85. Money Laundering, Extent of Money Laundering through Credit Card is Unknown, Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, United States Senate, 2002, GAO Document: GAO-02-670.
86. OECD Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL.
87. OECD Policy Guidance on Identity Theft, 2007.
88. Personal Information, Data Breaches are frequent, but evidence of resulting identity theft is limited; However, the full extent is unknown, Report to Congressional Requesters, 2007, GAO Document: GAO-07-737.
89. Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report to the Secretary-General, 2007, E/CN.15/2007/8/Add. 3.
90. Social Security Numbers, Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, Report to the Chairman, Subcommittee on Administrative Oversight and the Courts, Committee on the Judiciary, U.S. Senate, GAO Document: GAO-07-752.
91. Social Security Numbers, More could be done to protect SSNs, Statement of C. M. Fagnoni, Managing Director Education, Workforce and Income Security, Testimony Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives, 2006, GAO Document: GAO-06-586T.
92. Techniques of Identity Theft, CIPPIC Working Paper No. 2 (ID Theft Series), 2007.
93. The Use of Technology to Combat Identity Theft, Report on the Study Conducted Pursuant to Section 157 on the Fair and Accurate Credit Transaction Act of 2003, 2005, available at: [https://www.treasury.gov/offices/domestic-finance/financial-institution/cip/biometrics\\_study.pdf](https://www.treasury.gov/offices/domestic-finance/financial-institution/cip/biometrics_study.pdf) (last visited October 2008).
94. The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond”, page 4 et seq., available at: [http://www.antiphishing.org/reports/APWG\\_CrimewareReport.pdf](http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf) (last visited October 2008).
95. United Nations: Report of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, E/CN.15/2007/8 and Add. 1-3.







# TYOLOGY AND CRIMINALIZATION APPROACHES TO IDENTITY-RELATED CRIME: COMPENDIUM OF EXAMPLES OF RELEVANT LEGISLATION\*

**Gilberto Martins de Almeida**

**Martins de Almeida Advogados, Rio de Janeiro, Brazil**

---

\*The present Compendium was originally prepared for use as a working document at the fourth meeting of the core group of experts on identity-related crime, organized by the United Nations Office on Drugs and Crime and held in Vienna, Austria, on 18-22 January 2010. The opinions expressed in this Compendium are those of the author and do not reflect the views of the United Nations.



# Contents

	<i>Page</i>
I. INTRODUCTION .....	59
1. Purpose, scope and content of the Compendium .....	60
2. Terminology.....	62
II. MATRIX OF TYPOLOGY AND CRIMINALIZATION APPROACHES TO IDENTITY-RELATED CRIME .....	63
1. Identity-related crime legislation: definitions, means or format of identity-related information, protected ID information .....	63
2. Identity-related crime typologies: objective elements and classification of pertinent conducts.....	66
3. Identity-related crime typologies: subjective elements and requirements.....	67
III. COMPENDIUM OF EXAMPLES OF RELEVANT LEGISLATION .....	69
1. “Personal data” .....	69
2. “Personal status” .....	70
3. “Identity information” .....	70
4. “Means of identification” .....	71
5. “Identity document”, or “identification document” .....	71
6. Falsification and issuance or use of incorrect health certificates.....	73
7. False statement for passport.....	73
8. False passports and licenses for possession of weapons .....	74
9. Identification code.....	74
10. Identification marks .....	74
11. Genetic imprints.....	75
12. Misuse of electronic signature .....	75
13. Impersonation .....	76
14. Forgery of identification document.....	76
15. Forgery of identity in document delivered by public bodies .....	78
16. False document .....	78
17. Violation of personal data and websites.....	79
18. Skimming .....	79
19. Offences related to electromagnetic-records and electromagnetic record payment cards .....	81
20. Unauthorized use of credit card data .....	82

21. Identity theft .....	82
22. Computer-related identity theft.....	83
23. Preparation .....	83
24. Obtaining.....	84
25. Transfer .....	85
26. Use.....	86
27. Possession .....	87
28. Criminal misuse .....	87
29. Aggravating circumstances .....	88
30. Fraud/identity fraud.....	89
31. Intent to commit another offence .....	90
ANNEXES .....	92
A.1 Table 1—Identity-related crime legislation: definitions, means or format of identity-related information, protected ID information.....	92
A.2 Table 2—Identity-related crime typologies and categories of conducts .....	98
A.3 Table 3—Identity-related crime typologies: subjective elements and requirements .....	98
Samples of national laws, and relevant sources .....	100
Bibliography .....	103



# I. INTRODUCTION

Pursuant to Economic and Social Council (ECOSOC) resolution 2004/26, UNODC commissioned a study on “fraud and the criminal misuse and falsification of identity”, which was released in early 2007. The study’s approach was broad in three ways: first, the general term “identity-related crime” has been used to cover all forms of illicit conduct involving identity, including offences described, often not in a consistent manner, as “identity fraud” and “identity theft”; second, criminal acts related to identity theft were considered in their entirety to include their commission both online and offline, with more emphasis on sophisticated criminal schemes and patterns due to existing linkages to transnational organized crime and other criminal activities; and, third, identity-related crime was considered jointly with fraud given their close relationship and the specific directions of the ECOSOC mandate.

The findings of the study<sup>1</sup> were based on the information provided by 46 Member States, including many of the OECD Member States. The main contribution and achievement of that study was the consideration of the problem from a new criminal justice perspective and the treatment of identity abuses as distinct criminal offences, as opposed to the traditional approach of criminalizing other activities committed using false identities. The study also tackled differences and deviations in definitional and conceptual approaches at the national level with regard to the criminal misuse and falsification of identity and shed light on various aspects revealing the complexity of the problem and its criminal diversity.

Building upon the results and recommendations of the study and in accordance with its mandate arising from ECOSOC resolution 2007/20, UNODC launched a consultative platform on identity-related crime with the aim to bring together senior public sector representatives, business leaders, international and regional organizations and other stakeholders to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime. As a first step, a core group of experts was established to exchange views on the best course of action and the most appropriate initiatives that need to be pursued under the platform.

In all meetings of the core group, the experts agreed that the problems posed by identity-related crime are novel and require further work towards establishing appropriate classifications of the crime, founded on a basic typology or other frame of reference. The development of such a typology was seen by the group as an element that needs to be in place before considering the most suitable legislative responses to identity-related crime.

---

<sup>1</sup> The full text of the study is available at: <http://www.unodc.org/unodc/en/organized-crime/index.html#IDCRIME>.

In relation to these legislative responses, it was noted that, while several States are in the process of considering or establishing new criminal offences against identity abuses, others remain to be convinced that a new perspective on criminalization would be a sufficient improvement over existing offences such as fraud, forgery and impersonation. Thus, the group recommended that UNODC take action to raise awareness of the legal issues at stake and the policy options available in this regard.

The experts further agreed that another important role for UNODC would be the preparation of a range of materials to assist countries wishing to establish new criminal offences. Therefore one of the recommended approaches was for UNODC to develop materials, such as outlines of policy issues and options and general elements to consider when formulating offences, and outlines or descriptions of the sorts of conduct that could be criminalized.

On the recommendation of the Commission on Crime Prevention and Criminal Justice at its eighteenth session, the Economic and Social Council adopted resolution 2009/22 of 30 July 2009, in which the Council requested UNODC, in consultation with Member States and taking into account relevant intergovernmental organizations and, in accordance with the rules and procedures of the Economic and Social Council, experts from academic institutions, relevant non-governmental organizations and the private sector, to collect, develop and disseminate, among others, “material and guidelines on the typology of identity-related crime and on relevant criminalization issues to assist Member States, upon request, in the establishment of new identity-based criminal offences and the modernization of existing offences, taking into account the pertinent work of other intergovernmental organizations engaged in related matters”.

The present Compendium was prepared in line with the above directions and guidelines. Its draft was presented at the fourth meeting of the core group of experts on identity-related crime (Vienna, 18-22 January 2010) for its review and approval.

## 1. Purpose, scope and content of the Compendium

The primary purpose of this Compendium is to provide an inventory of countries’ national legal provisions which are specific to identity-related crime, or which may concern it.

Such compilation has the ultimate objective to apportion practical information which may be of interest for development of further studies or for production of technical assistance manuals and training.

This Compendium does not purport to offer deeper comments or analysis on the panorama portrayed, or on any specific topic. Prior papers<sup>2</sup> presented at the core group of experts shall be consulted for reference in this regard.

---

<sup>2</sup> Especially the paper on “Legal Approaches to Criminalize Identity Theft”, prepared by Dr Marco Gercke, and submitted to Commission on Crime Prevention and Criminal Justice at its eighteenth session (Vienna, 16-24 April 2010) (see E/CN.15/2009/CRP.13).

In addition, the present compilation does not purport to reproduce, with respect to any topic herein addressed, every relevant legal provision existing in the countries researched. It rather purports to be used as a mosaic picturing a number of domestic legislative approaches to different forms of identity-related crime. Thus, the resulting overview provides a panorama of legislation of countries from different regions and portrays diverse national experiences and profiles.

For similar reasons, the scope of this Compendium does not include the design of a systematic conceptual approach regarding identity-related crime due to the great diversity of national approaches in this field.

The content of this Compendium builds upon prior work of the core group of experts, updating and expanding it so to address any identity-related crime, beyond identity theft, and was carried out by means of: (a) a questionnaire sent in December 2009 to participants of the core group, (b) discussions held during the fourth meeting of the core group, and (c) resort to latest legal-technical literature, including publications in the field as recently as 2009, as indicated in the bibliography.

It is important to mention that although the data on all countries researched were inserted, for graphic reasons, in the annex tables (annex tables A.1, A.2 and A.3) they belong to different research occasions, and are originated from different sources.

Research on the following countries took into account information/data as of December 2009: Argentina, Australia, Austria, Bolivia (Plurinational State of), Brazil, Canada, Chile, Colombia, Costa Rica, Croatia, Ecuador, Finland, France, Germany, Hungary, India, Italy, Japan, Latvia, Mexico, Nigeria, Norway, Peru, Portugal, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States of America and Venezuela.

Research on the following countries took into account information/data as of September 2010: Albania, Armenia, Azerbaijan, Bahrain, Barbados, Botswana, Bulgaria, Canada, China, Cyprus, Czech Republic, Egypt, Estonia, Georgia, Indonesia, Iraq, Ireland, Jamaica, Kazakhstan, Kuwait, Kyrgyzstan, Lithuania, Malaysia, Oman, Philippines, Qatar, Republic of Moldova, Russian Federation, Singapore, Syrian Arab Republic, Tajikistan, the Former Yugoslav Republic of Macedonia, United Arab Emirates, Ukraine, Uzbekistan and Yemen.

The Compendium also took into account information from UNODC obtained in response to a “Questionnaire on Fraud and Criminal Misuse and Falsification of Identity” which was circulated in 2006 for the purposes of compiling material for the United Nations study on “fraud and the criminal misuse and falsification of identity”. Such information referred to the following countries: Belarus, Croatia, Finland, Germany, Greece, Hungary, Italy, Japan, Jordan, Latvia, Lebanon, Mauritius, Morocco, Netherlands, Norway, Republic of Korea, Romania, Russian Federation, Saudi Arabia, Slovakia, Slovenia, Sweden, Switzerland, Turkey, United Kingdom and United States of America.

All available data have been verified up to 29 September 2010.

The wording of legal provisions quoted as samples in chapter III have been accompanied by indication of relevant sources of information, as well as of the literature or web pages where they can be found.

Annex tables A.1, A.2 and A.3 feature countries' laws, which were found to contain identity-related provisions.

The column "Legislation" in the tables was filled in where provisions specific to identity-related crime were found through the research, whereas the other columns in the tables were filled in where generic provisions were found. No information in the columns indicates that neither legislation nor specific identity-related provisions were detected within the limits of this work.

The addition of a higher number of countries to the research, as well as further completion, validation and update of fields in the tables,<sup>3</sup> including the mapping of all sorts of applicable national laws, beyond the ones researched in this work, such as national criminal codes and cybercrime and privacy statutory laws, may require that a comprehensive questionnaire be sent, ideally in the name of the United Nations, to a greater number of addressees.

## 2. Terminology

The terminology used in this Compendium has been defined and explained in prior literature and papers commissioned by UNODC. Nevertheless, some samples of legal provisions quoted herein contain definition of some types of crime, or of some elements which integrate relevant typology.

---

<sup>3</sup> Including the mapping of all sorts of applicable national laws, beyond the ones researched within the context of the current work (which included, mainly, research of cybercrime laws and of privacy laws).



## II. MATRIX OF TYPOLOGY AND CRIMINALIZATION APPROACHES TO IDENTITY-RELATED CRIME

This chapter outlines the positive statistical results of the research, which are graphically displayed in the annex tables (A.1, A.2 and A.3). The number of countries mentioned in the statistics reflect the number of fields filled in with “Yes” in the respective columns of the tables. The notes which accompany each topic below are not aimed at establishing scientific findings or conclusions, and rather envisage solely to highlight areas which may deserve specific attention.

### 1. Identity-related crime legislation: definitions, means or format of identity-related information, protected ID information

#### *Diversity of statutory laws including definitions of identity-related information*

With regards to the different types of legislation which deal with definitions of identity-related information, the research indicated the following results:

- Definitions in Criminal Codes: 24 countries (Albania, Argentina, Austria, Azerbaijan, Brazil, Bulgaria, China, Colombia, Ecuador, Estonia, France, Georgia, Germany, Italy, Japan, Kazakhstan, Mexico, Nigeria, Peru, Spain, Switzerland, Sweden, Turkey, United States of America).
- Definitions in privacy laws: 2 countries (Australia, Russian Federation).
- Definitions in Information Technology laws: 1 country (India).
- Definitions in other laws: 14 countries (Bolivia (Plurinational State of), Canada, Chile, Costa Rica, France, Hungary, Japan, Philippines, Portugal, Republic of Moldova, Romania, South Africa, United Kingdom, Venezuela).

Although most definitions are found in national Criminal Codes, an expressive number of definitions have been included in laws which deal with miscellaneous subject matters. This seems to reflect the great diversity of perceptions on identity-related crime.

It is also worth mentioning that the number of definitions which have been adopted in either privacy or information technology laws is relatively small. This seems to point to the fact that most countries researched have seen identity-related crime as not substantively attached to privacy or technology.

### *Diversity of terms employed in definitions of identity-related information*

With regard to the different options of terminology employed in definitions of identity-related information, the research indicated the use of varying terms, as follows:

- “Personal” data, information, database, or document: 14 countries (Argentina, Australia, Austria, Bulgaria, Colombia, Ecuador, Estonia, Hungary, Peru, Republic of Moldova, Russian Federation, South Africa, Spain, Venezuela).
- “Computer” or “system” data, or similar expressions referring to technology: 10 countries (Azerbaijan, Bolivia (Plurinational State of), Chile, Georgia, Italy, Japan, Kazakhstan, Kyrgyzstan, Nigeria, Romania).
- “Secrets”, or “confidential data”: 2 countries (Costa Rica, Portugal)
- “Data”: 2 countries (France, Sweden).
- “Identity information”, “identity document”, “identities”, “identification cards”, or “identification paper”: 7 countries (Albania, Canada, China, Germany, India, Mexico, Philippines).

Most provisions rely on the “personal” character of information as the main component to qualify identity information, closely followed by the “technological” aspect of such kind of information. This draws attention to the assumption that identity-related information is highly affected by digital phenomena, and further raises the question whether the main focus in typology should concentrate on the intrinsic identity aspect of the related crimes, or whether the latter should be absorbed, to some extent, by the specificities of technology-related matters.

The fact that many countries have qualified identity-related crime under the generic and ambiguous umbrella of “personal”, as an adjective, seems to indicate that although identity-related crimes represent nowadays an important (and increasing) number of crimes, most researched countries have not yet developed awareness on the convenience of regulating identity-related crimes in a more specific fashion.

The small number of references to “identity” information or to “identification” paper is only comparable to the few references to secrecy. This seems to indicate that identity has not often been perceived as something to be dissociated from “personal” (and perhaps more specifically, from privacy) aspects.

### *Diversity of format or means of identity-related information*

With regard to the different kinds of format or means of identity-related information, the research has indicated the following results:

- Any format or means: 11 countries (Albania, Australia, Austria, Bulgaria, Canada, China, France, Hungary, India, Nigeria, South Africa).
- Electronic format or means: 20 countries (Argentina, Azerbaijan, Bolivia (Plurinational State of), Chile, Colombia, Costa Rica, Ecuador, Estonia, Georgia, Italy,

Japan, Kazakhstan, Kyrgyzstan, Mexico, Peru, Philippines, Republic of Moldova, Russian Federation, Spain, Venezuela).

- Documental means: 4 countries (Brazil, Germany, Turkey, United Kingdom).

The association between identity-related information and electronic means appears again as a very strong one, exceeding by far the number of references to documental means of storage.

Considering that identity-related crime may be perpetrated not only through electronic means (for instance, crimes relating to “physical” forgery or misappropriation of passports), it seems to be of interest to investigate whether the focus on the connection of identity-related information with electronic means is proportionate to the focus on its connection with other sorts of format or means.

### *Diversity of identity-related information protected by national laws*

With regard to the different types of identity-related information or documents protected by national laws, the research indicated the following results:

- Social Security number, single PIN number, or health insurance number: 9 countries (Albania, Argentina, Austria, Canada, Chile, Italy, South Africa, Spain, United States of America).
- Name, address, date of birth, or written signature: 4 countries (Albania, Argentina, Canada, South Africa).
- Birth, marital status, death certificate, ID card, passport, or immigration document: 6 countries (Albania, Brazil, Canada, Germany, South Africa, United Kingdom).
- Driver’s license, military status card, voter card for political elections: 6 countries (Brazil, Canada, Germany, South Africa, United Kingdom, United States of America).
- Credit or debit card number, or financial institution account number: 5 countries (Canada, Japan, South Africa, United Kingdom, United States of America).
- E-mail login, e-mail or web browsing passwords, mac-address or IP-address, electronic or digital signature, or username: 4 countries (Canada, India, Japan, United States of America).
- Fingerprint, voice print, retina image, iris image, or DNA profile: 2 countries (Canada, South Africa).

In the sampling above, the number of non-electronic identity-related information is greater than the number of the purely electronic one. This seems, at first sight, to contradict the finding on the prevailing connection between identity-related information and electronic means. However, it is important to notice that even documents not originally electronic (social security card, passport, etc.) are often produced or reproduced through the use of electronic means, and may therefore be subject to electronic misappropriation (of its

image, or of relevant data or information). In other words, some elements of an electronic identity-related crime may be present even when the document targeted by the criminal is not originally (or typically) electronic.

Furthermore, the digital representation of newer forms of personal identification (such as retina image, iris image, or DNA profile) which are likely to be increasingly targeted by criminals reinforces the connection between electronic means and identity-related information.

## 2. Identity-related crime typologies: objective elements and classification of pertinent conducts

With regard to typologies of identity-related crime focusing on objective elements of pertinent conducts, the findings of the research indicated the following classification:

### *Production of counterfeit document or falsification of genuine document*

The following countries contemplated such sort of typology in their national laws: Albania, Argentina, Brazil, Germany, Japan, South Africa, United Kingdom, United States of America.

### *Individual unlawful use of identity-related information*

The following countries contemplated such sort of typology in their national laws: Albania, Argentina, Brazil, Canada, Germany, India, Japan, South Africa, United Kingdom, United States of America. Pertinent conducts included, inter alia, the possession, use, holding, obtaining, control, procurement of identity-related information, as well as illegal access to such information.

### *Collective unlawful use of identity-related information*

The following countries contemplated such sort of typology in their national laws: Albania, Argentina, Brazil, Canada, Germany, Japan, South Africa, United Kingdom, United States of America. Pertinent conducts included, inter alia, the transferring, making available or placing online, transmission, distribution, sale or supply, offering for sale or supply (or possession for such purposes) and dissemination of identity-related information.

### *Trafficking in identity-related information*

The following countries contemplated such sort of typology in their national laws: Argentina, Germany, South Africa. Pertinent conducts included, inter alia, the

transferring, transportation, disposal (or having or obtaining control with such an intent) and storing of identity-related information, as well as undertaking to import or export such information.

#### *Damage to third party's identity-related information*

The following countries contemplated such sort of typology in their national laws: Brazil, Germany, South Africa. Pertinent conducts included, inter alia, provoking or affirming a mistake, deception by means of pretending that false facts exist, destroying, occulting, distorting or suppressing true facts, and influencing the result of a data processing operation.

#### *Attempting/conspiring/aiding/abetting*

The following countries contemplated such sort of typology in their national laws: Germany, Japan, South Africa, United States of America.

### 3. Identity-related crime typologies: subjective elements and requirements

With regard to the varying subjective elements and requirements of identity-related crimes, the research indicated the following results:

#### *Intent to commit, aid, or abet unlawful activity*

Found in five countries: Argentina, Canada, Germany, South Africa, United States of America.

#### *Intent to defraud*

Found in seven countries: Argentina, Brazil, Canada, Germany, India, United Kingdom, United States of America.

#### *Intent to deceive*

Found in eight countries: Argentina, Brazil, Canada, Germany, India, Japan, South Africa, United States of America.

#### *Intent to obtain for oneself or a third person unlawful material benefit or advantage*

Found in three countries: Brazil, Germany, South Africa.

#### *Intent to use document for establishing registrable facts about oneself*

Found in one country: United Kingdom.

#### *Awareness, belief, or recklessness as to obtaining or possessing someone else's identity information*

Found in one country: Canada.

*Awareness, belief, or recklessness as to the falseness or improper obtaining of the document*  
Found in one country: United Kingdom.

*Awareness, belief, or recklessness as to whether the information will be used to commit an indictable offence*  
Found in two countries: Canada, United Kingdom.

The above indicates that intent is required in many countries that have enacted legislation addressing identity-related crime. In contrast, awareness, belief and recklessness are present only in a few countries, within such sampling. Given the “volatile” nature of information stored in electronic databases, a question remains open on whether, and to what extent, the element of intent is expected to be required, or whether, and to what extent, some presumption of intent would be admissible in light of certain circumstances.

# III. COMPENDIUM OF EXAMPLES OF RELEVANT LEGISLATION

This chapter presents samples of provisions contemplated in national laws of the countries researched. The notes which introduce some topics below are not aimed at describing or analyzing the provisions at hand, and rather solely purport to highlight aspects which may deserve specific study.

## 1. “Personal data”

The protection of identity-related information is often regulated in the context of privacy laws. Although privacy protection concentrates mainly on the acts which may characterize privacy invasion, it may contemplate some definitions which also relate to identity-related information—for instance, the concept of “personal data” may comprise not only certain given attributes associated with certain individual (usually denominated “special data”), but also some data which may make that individual identified or identifiable.

Hungary, Act LXIII of 1992, on the protection of personal data and on the disclosure of data of public interest:

1. Personal data—shall mean any data relating to a specific (identified or identifiable) natural person (hereinafter referred to as ‘data subject’) as well as any conclusion with respect to the data subject which can be inferred from such data. In the course of data processing such data shall be considered to remain personal as long as their relation to the data subject can be restored.
2. Special data—shall mean any personal data relating to:
  - (a) racial, or national or ethnic minority origin, political opinion or party affiliation, religious or ideological belief, or membership in any interest representing organisation;
  - (b) state of health, pathological addictions, sexual life or personal data pertaining to criminal records [...]

Germany, Federal Data Protection Act,<sup>4</sup> Section 3, items 1 and 9:

- 1) “Personal data” means any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)”.

[...]

<sup>4</sup> Federal Data Protection Act of 1 January 2002, see: [http://www.bdd.de/Download/bdsg\\_eng.pdf](http://www.bdd.de/Download/bdsg_eng.pdf).

9) “Special categories of personal data” means information on a person’s racial and ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life.

Sweden, Personal Data Act, Section 3:<sup>5</sup>

Personal data—All kinds of information that directly or indirectly may be referable to a natural person who is alive.

## 2. “Personal status”

Data on the “personal status” of an individual are directly or indirectly linked to relevant identity data, unless the former is kept only for purposes of statistics and the latter is eliminated. Whenever identity data are maintained, and the link with personal status is not protected (for instance, by means of granting a randomly allocated code), data on personal status may be qualified as identity-related information.

Germany, Criminal Code,<sup>6</sup> Section 169, Falsification of Personal Status:

- 1) Whoever declares a child to be somebody else or falsely gives or suppresses the personal status of another to a public authority responsible for the maintenance of personal status registers or the determination of personal status, shall be liable to imprisonment of not more than two years or a fine.
- 2) The attempt shall also be punishable.

## 3. “Identity information”

There are different sources of identification of a person, which may characterize the so-called “identity information”. Identity information relates to the contents of information, irrespectively of where it is recorded, vehicled, or stored.

Canada, Bill S-4 amending the Criminal Code (identity theft and related misconduct), Section 402.1:

402.1 For the purposes of sections 402.2 and 403, “identity information” means any information—including biological or physiological information—of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, such as a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, username, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver’s license number or password.

<sup>5</sup> Sweden Personal Act 1998:204, issued on 29 April 1998, see <http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf>.

<sup>6</sup> German Criminal Code in the version promulgated on 13 November 1998, *Federal Law Gazette [Bundesgesetzblatt]* I page 3322, last amended by Article 3 of the Law of 2 October 2009, *Federal Law Gazette I* page 3214, see: [http://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#StGBengl\\_000P169](http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169).



## 4. “Means of identification”

The nature of the expression “means of identification” is self-explanatory, but there are definitions of it, and its application may present interesting examples.

United States, 18 USC Section 1028, Chapter 47, Fraud and False Statements:

- 7) The term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:
- (a) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
  - (b) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
  - (c) unique electronic identification number, address, or routing code; or
  - (d) telecommunication identifying information or access device (as defined in section 1029(e)) [...]

## 5. “Identity document”, or “identification document”

The kinds of documents which may contain identity information are of interest to laws on identity-related crime, as they exemplify, or circumscribe, the hypotheses subject to enforcement of such laws. The wording of relevant provisions may combine a generic statement (on the purpose of the document) and a specific listing of documents.

United Kingdom, Identity Cards Act,<sup>7</sup> Section 26:

- 1) In Section 25 “identity document” means any document that is or purports to be:
- An ID card;
  - A designated document;
  - An immigration document;
  - A United Kingdom passport [...];
  - A passport issued by or on behalf of the authorities of a country or territory outside the United Kingdom or by or on behalf of an international organization;
  - A document that can be used (in some or all circumstances) instead of a passport;

<sup>7</sup> Identity Card Act of 2006, see: [http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga\\_20060015\\_en.pdf](http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf).

- A United Kingdom driving license; or
- A driving license issued by or on behalf of the authorities of a country or territory outside the United Kingdom.

United States, 18 USC Section 1028, Chapter 47, Fraud and False Statements:

3) the term “identification document” means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals [...]

Germany, Criminal Code,<sup>8</sup> Section 273, Modification of Official Identification Documents:

1) Whoever for the purpose of deception in legal commerce:

(a) removes, renders unrecognisable, covers up or suppresses an entry in an official identity document or removes a single page from an official identity document; or

(b) uses an official identity document altered in such a way;

shall be liable to imprisonment of not more than three years or a fine unless the offence is punishable under section 267 or section 274.

2) The attempt shall be punishable.

Canada, Bill S-4 amending the Criminal Code (identity theft and related misconduct), Section 56.1:

Identity documents (1) Every person commits an offence who, without lawful excuse, procures to be made, possesses, transfers, sells or offers for sale an identity document that relates or purports to relate, in whole or in part, to another person.

[...]

Definition of “identity document” (3) For the purposes of this section, “identity document” means a Social Insurance Number card, a driver’s license, a health insurance card, a birth certificate, a death certificate, a passport as defined in subsection 57(5), a document that simplifies the process of entry into Canada, a certificate of citizenship, a document indicating immigration status in Canada, a certificate of Indian status or an employee identity card that bears the employee’s photograph and signature, or any similar document, issued or purported to be issued by a department or agency of the federal government or of a provincial or foreign government.

<sup>8</sup> German Criminal Code in the version promulgated on 13 November 1998, *Federal Law Gazette [Bundesgesetzblatt]* I page 3322, last amended by Article 3 of the Law of 2 October 2009, *Federal Law Gazette I* page 3214; see [http://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#StGBengl\\_000P169](http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169).

## 6. Falsification and issuance or use of incorrect health certificates

There are some documents which, due to the importance of their contents, have deserved special attention on the part of legislators, concerning identity-related crime. One of such documents is the health certificate, which falsification, and issuance or use of incorrect ones has been addressed specifically.

Germany, Criminal Code,<sup>9</sup> Section 277, Falsification of Health Certificates:

Whoever using the title of physician or of another registered medical practitioner without having the right to do so, or illegitimately using the name of such persons, issues a certificate relating to his own state of health or that of another, or falsifies a genuine certificate of that type, and makes use of it in order to deceive public authorities or insurance companies shall be liable to imprisonment of not more than one year or a fine.

Ibid., Section 278, Issuing Incorrect Health Certificates:

Physicians and other registered medical practitioners who intentionally and knowingly issue an incorrect certificate relating to the state of health of a person for use with a public authority or insurance company shall be liable to imprisonment of not more than two years or a fine.

Ibid., Section 279, Use of Incorrect Health Certificates:

Whoever, in order to deceive a public authority or an insurance company about his own state of health or that of another, makes use of a certificate of the type indicated in section 277 and section 278, shall be liable to imprisonment of not more than one year or a fine.

## 7. False statement for passport

Serious consideration in many jurisdictions was given to issues related to safeguarding the integrity of passports. Some national provisions address false information provided for the issuance of passports.

Nigeria, Criminal Code,<sup>10</sup> Section 190A:

Any person who for the purpose of procuring a passport, whether for himself or any other individual, makes or causes to be made in any written application to a public officer a statement which to the knowledge of such person is false in any material particular is guilty of an offence, and is liable to imprisonment for one year.

<sup>9</sup> German Criminal Code in the version promulgated on 13 November 1998, Section 277, *Federal Law Gazette [Bundesgesetzblatt]* I page 3322, last amended by Section 3 of the Law of 2 October 2009, *Federal Law Gazette* I p. 3214, see: [http://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#StGBengl\\_000P169](http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169).

<sup>10</sup> Nigerian Criminal Code, of 1990, Chapter 18, see: [http://www.nigeria-law.org/Criminal%20Code%20Act-Part III-IV.htm](http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20III-IV.htm).

## 8. False passports and licenses for possession of weapons

Some country national laws have addressed false passports in conjunction with false license for possession of weapons.

Chile, Criminal Code,<sup>11</sup> Sections 199 and 200:

The public employee who issues a passport or license for possession of weapons under fabricated name or leaves it blank, shall be convicted for the penalty of imprisonment [...]

The one who makes a false passport or license for possession of weapons shall be punished with an imprisonment [...]. The same penalties shall apply to the ones who modify, in a truthful passport or license for possession of weapons, the name of the person to whom it was granted, or the name of the authority who issued it, or any other special circumstance.

## 9. Identification code

Identity information may be simply a code, which can identify someone. Such a code may be available in an “intangible” form (for instance, electronically) or be embedded in a device (for instance, in a token) associated with the purpose of accessing some equipment.

Japan, Unauthorized Computer Access Law,<sup>12</sup> Article 4:

No person shall provide another person’s identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer’s specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.

## 10. Identification marks

Some national laws have described identification marks and addressed illicit patterns of conduct associated with them.

<sup>11</sup> Chilean Penal, of 12 November 1874, Sections 199 and 200, see: <http://www.servicioweb.cl/juridico/Codigo%20Penal%20de%20Chile%20libro2.htm>.

<sup>12</sup> Law No. 128, of 1999.

Hungary, Criminal Code,<sup>13</sup> Section 277/A, Counterfeiting of Individual Identification Marks:

“Identification marks” are signs which may identify a person as being characteristic of the body of that person or being incorporated by that person into a document (for instance, the fingerprint of a person on a passport).

1) Any person who:

- (a) removes, or counterfeits in some other way, an individual identification mark,
- (b) acquires or uses an article whose individual identification mark is counterfeit or forged, or whose individual identification mark has been removed, commits a felony offense and shall be punishable with imprisonment of up to three years.

2) The punishment shall be imprisonment of up to five years if the crime described in Subsection (1) is committed:

- (a) in a business-like manner, or
- (b) as part of a criminal conspiracy.

## 11. Genetic imprints

The DNA code of a person can identify him/her, and is therefore subject to protection against undue discovery, access or disclosure. Even the research of genetic imprints is criminalized, when it does not serve medical or scientific purposes.

France, Criminal Code,<sup>14</sup> Articles 226-28:

Researching the identification of a person through his genetic imprints for purposes neither medical nor scientific, or other than in an inquiry or investigation made in the course of judicial proceedings, is punished by one year imprisonment and a fine of €15,000.

The same penalty applies to the disclosure of information concerning the identification of a person through his genetic imprints or proceeding to the identification of a person through his genetic imprints without holding the authorisation provided for under article L. 145-16 of the Public Health Code.

## 12. Misuse of electronic signature

Due to their special security features, electronic signature provides a strong presumption that its user is actually the person he/she is said to be. As a consequence, misuse of electronic signature is criminalized.

<sup>13</sup> Act No. LXIII of 1992, see: <http://abiweb.obh.hu/adatved/indexek/AVTV-EN.htm>.

<sup>14</sup> French Penal Code, Act No. 1994-653, of 29 July 1994, Article 8, Official Journal of 30 July 1994; Ordinance No. 2000-916 of 19 September 2000, Article 3, Official Journal of 22 September (came into force on 1 January 2002).

India, Information Technology Act,<sup>15</sup> Section 66C, Punishment for identity-related crime:

Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to rupees one lakh.

### 13. Impersonation

Impersonation is the use of someone else's identity to deceive third parties making them believe that one is the person he pretends to be.

Nigeria, Criminal Code,<sup>16</sup> Sections 484 and 485:

Any person who, with intent to defraud any person, falsely represents himself to be some other person, living or dead, is guilty of a felony, and is liable to imprisonment for three years. If the representation is that the offender is a person entitled by will or operation of law to any specific property and he commits the offence to obtain such property or possession thereof, he is liable to imprisonment for fourteen years.

Any person who, without lawful authority or excuse, the proof of which lies on him, makes, in the name of any other person, before any court or person lawfully authorized to take such an acknowledgment, an acknowledgment of liability of any kind, or an acknowledgment of a deed or other instrument, is guilty of a felony, and liable to imprisonment for seven years.

### 14. Forgery of identification document

Beyond undue obtaining or improper use of identity information, the action of falsifying a document destined to certify the identity of a person may be a crime in itself.

Argentina, Criminal Code,<sup>17</sup> Section 292:

[...] If the falsified or modified document is destined to certify the identity of persons or the ownership or license for driving automobiles, the penalty shall be of three to eight years.

Norway, Criminal Code,<sup>18</sup> Sections 179 and 182:

By documents is meant in this code any object that in writing or otherwise contains a statement that is either of significance as evidence of any right, obligation or exemption therefrom or appears to be designed to serve as evidence.

<sup>15</sup> Information Technology (Amendment) Act, of 2008.

<sup>16</sup> Nigerian Criminal Code of 1990, see: <http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm>

<sup>17</sup> As amended by Federal Law No. 24.410/95.

<sup>18</sup> Norwegian Criminal Code, Act of 22 May 1902 No. 10, see: <http://www.ub.uio.no/ujur/ulovdata/lov-19020522-010-eng.pdf>.

Any person who with unlawful intent uses as genuine or unfalsified any document that is forged or falsified, or who is accessory thereto, shall be liable to fines or imprisonment for a term not exceeding two years, but not exceeding four years if the document in question is a Norwegian or foreign official document. If the document has been used with the intent of obtaining evidence for a lawful claim or for protection against an unlawful claim, fines or imprisonment for a term not exceeding one year may be imposed.

Finland, Criminal Code,<sup>19</sup> Chapter 16, Section 5, Offences against the public authorities:

A person who in order to mislead a public authority provides a false name or otherwise provides false or misleading information on his/her identity, or for this purpose uses another person's identity card, passport, driver's license or other such certificate, shall be sentenced for false identity to a fine or to imprisonment for at most six months.

Ibid., Chapter 33, Forgery offences, Section 1, Forgery (769/1990):

A person who prepares a false document or other item or falsifies such a document or item in order for it to be used as misleading evidence or uses a false or falsified item as misleading evidence shall be sentenced for forgery to a fine or imprisonment for at most two years. An attempt is punishable.

Latvia, Penal Code,<sup>20</sup> Section 177:

(1) For a person who deliberately enters false data into an automated data processing system for the acquisition of the property of another person or the rights to such property, or the acquisition of other material benefits, in order to influence the operation of the resources thereof (computer fraud), the applicable sentence is deprivation of liberty for a term not exceeding five years or a custodial arrest, or community service, or a fine not exceeding eighty times the minimum monthly wage.

(2) For a person who commits computer fraud, if commission thereof is repeated, or by a group of persons pursuant to prior agreement, the applicable sentence is deprivation of liberty for a term not exceeding eight years or with confiscation of property, or a fine not exceeding one hundred and fifty times the minimum monthly wage.

(3) For a person who commits computer fraud, if it has been committed on a large scale, the applicable sentence is deprivation of liberty for a term of not less than eight years and not exceeding fifteen years, or a fine not exceeding two hundred times the minimum monthly wage, with or without confiscation of property.

<sup>19</sup> Finnish Criminal Code (39/1889, amendments up to 940/2008 included), Section 5, *Giving false identifying information* (563/1998), see: <http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf>.

<sup>20</sup> Latvian Penal Code, Law of 12 February 2004, Chapter XVIII Criminal Offences against Property, Section 177, see: <http://www.legislationline.org/download/action/download/id/1683/file/4b5d86c3826746957aa400893abc.htm/preview>.

## 15. Forgery of identity in document delivered by public bodies

Particular attention has been given by legislators to the circumstances under which a forged document was issued by a public body.

France, Criminal Code,<sup>21</sup> Article 441-2:

Forgery committed in a document delivered by a public body for the purpose of establishing a right, an identity or a capacity, or to grant an authorisation is punished by five years' imprisonment and a fine of €75,000.

## 16. False document

The definition of false document may be instrumental for the concept of falsification of a document, inclusively where it relates to false identity.

Nigeria, Criminal Code,<sup>22</sup> Section 464:

A document or writing is said to be false:

[...]

(c) if the whole or some material part of the document or writing purports to be made by or on behalf of some person who does not, in fact, exist; or

(d) if the document or writing is made in the name of an existing person, either by that person himself or by his authority, with the fraudulent intention that it should pass as being made by some person, real or fictitious, other than the person who makes it or authorizes it to be made.

Turkey, Criminal Code,<sup>23</sup> Article 157:

A person who by means of trickery behaviours and to the detriment of others, deceives someone to obtain wrongful benefit for himself or for another person shall be sentenced to imprisonment for a term of one to five years and to a heavy fine of five thousand days.

Croatia, Criminal Code,<sup>24</sup> Article 224a, Computer Fraud:

(1) Whoever, with an aim to procure unlawful pecuniary gain for himself or a third party, enters, uses, alters, deletes or renders unusable electronic data or computer programmes or disables or hampers the work or use of the computer system or

<sup>21</sup> Ordinance No. 2000-916 of 19 September 2000, Article 3, Official Journal of 22 September 2000 (came into force on 1 January 2002).

<sup>22</sup> Nigerian Criminal Code, of 1990, Chapter 43, Section 464, see: <http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20to%20the%20end.htm>.

<sup>23</sup> Croatian Criminal Code, Law No. 5237, passed on 26.09.2004 (*Official Gazette* No. 25611, dated 12.10.2004); see: <http://www.legislationline.org/documents/action/popup/id/6872/preview>.

<sup>24</sup> The Official Gazette of the Republic of Croatia, "*Narodne novine*", No. 110 of 21 October 1997 (entered into force on 1 January 1998), see: [http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation\\_\\_Criminal-Code.pdf](http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Code.pdf).



programme causing thereby damage to another shall be punished by imprisonment from six months to five years.

(2) Whoever commits the criminal offence referred to in paragraph 1 solely with the purpose of causing damage to another shall be punished by imprisonment from three months to three years.

(3) Whoever, without authorization, produces, procures, sells, possesses or makes accessible to another special devices, equipment, computer programmes or electronic data created and adapted for the perpetration of the criminal offences referred to in paragraphs 1 or 2 of this Article shall be punished by a fine or by imprisonment not exceeding three years.

(4) Special devices, equipment, electronic data or computer programmes created, used or adapted for the perpetration of criminal offences that were used to perpetrate the criminal offence referred to in paragraph 1 and 2 of this Article shall be forfeited.

(5) Whoever attempts to perpetrate the criminal offence referred to in paragraph 2 and 3 of this Article shall be punished.

## 17. Violation of personal data and websites

As mentioned before, personal data and personal codes may represent identity information. Although identity-related crime is not necessarily grounded on privacy concerns, violation of personal data and codes may imply improper obtaining or use of identity information.

Chile, Criminal Code,<sup>25</sup> Sections 269F and 269G:

*Violation of personal data.* The one who, not being authorized for that, obtains, compiles, discloses, modifies or employs personal codes or personal data contained in files, archives, databases or similar media, for own benefit or of third parties, shall be convicted for imprisonment of forty-eight to ninety-six months [...].

*Invasion of websites to capture personal data.* The one who, with illicit aim and not being authorized for that, designs, develops, trades, sells, performs, programmes or sends web pages, links or frames, shall be convicted for imprisonment of forty-eight to ninety-six months [...].

## 18. Skimming

Skimming is the practice of capturing personal data stored in electromagnetic records, such as, for example, the magnetic strip of credit cards, by means of use of small devices, which are capable of scanning such magnetic strip.

<sup>25</sup> Chilean Penal Code, of 12 November 1874, Sections 269F and 269G, see: <http://www.servicioweb.cl/juridico/Codigo%20Penal%20de%20Chile%20libro2.htm>.

Japan, Law No. 128 of 1999,<sup>26</sup> Article 161-2, Illegal Production of Electromagnetic Record:

1. A person who, with the intent to bring about improper administration of affairs of another person, unlawfully produces an electromagnetic record which is for the use of the administration of such affairs and is related to right, duty or certification of fact, shall be punished by *choeki* for not more than 5 years or a fine of not more than 500,000 yen.
2. When the crime prescribed in the preceding paragraph is committed against an electromagnetic record which should be prepared by a public office or a public officer, the offender shall be punished by *choeki* for not more than 10 years or a fine of not more than 1,000,000 yen.
3. A person who, with such intent specified in paragraph 1, puts an unlawfully produced electromagnetic record related to right, duty or certification of fact in use for the administration of affairs of another person shall be punished by the same penalty as prescribed for a person who unlawfully produced such an electromagnetic record.
4. Attempts of the crime prescribed in the preceding paragraph shall be punished.

Japan, Criminal Code,<sup>27</sup> Article 163-2, Illegal Production of Electromagnetic-Record Payment Cards:

1. A person who, for the purpose of causing improper administration of financial affairs of another person, unlawfully produces an electromagnetic record which is for the use of such administration and composes a credit card or other payment card for prices or charges, shall be punished by *choeki* for not more than 10 years or a fine of not more than 1,000,000 yen. The same shall apply to a person who unlawfully produces an electromagnetic record which composes a cash card for the withdrawal of money.
2. A person who, for the purpose specified in the preceding paragraph, puts an unlawfully produced electromagnetic record specified in the same paragraph in use for the administration of financial affairs of another person, shall be dealt with in the same way prescribed in the same paragraph.
3. A person who, for the purpose specified in paragraph 1, transfers, lends or imports a card composed of an unlawful electromagnetic card specified in the same paragraph, shall be dealt with in the same way prescribed in the same paragraph.

---

<sup>26</sup> Unauthorized Computer Access Law (Law No. 128, of 1999), see: <http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf>.

<sup>27</sup> Act No. 45, of 1907.

## 19. Offences related to electromagnetic-records and electromagnetic record payment cards

Japan, Criminal Code, Article 163-3, Possession of Illegal Electromagnetic-Record Payment Cards:

1. A person who, for the purpose specified in paragraph 1 of the preceding paragraph, possesses the card specified in paragraph 3 of the same paragraph shall be punished by *choeki* for not more than 5 years or a fine of not more than 500,000 yen.

Ibid., Article 163-4, Preparation for Illegal Production of Electromagnetic-Record Payment Cards:

1. A person who, for the purpose of making use of the action specified in paragraph 1 of Article 163-2, obtains the information for an electromagnetic records specified in the same paragraph, shall be punished by *choeki* for not more than 3 years or a fine of not more than 500,000 yen. The same shall apply to a person who, knowing the purpose of the obtainer, provides the information.
2. A person who, for the purpose specified in the preceding paragraph, keeps the illegally obtained information of an electromagnetic record specified in paragraph 1 of Article 163-2 shall be dealt with in the same way prescribed in the preceding paragraph.
3. A person, who, for the purpose specified in paragraph 1, prepares instruments or materials, shall be dealt with in the same way prescribed in the same paragraph.

Argentina, Federal Law No. 25.830, Section 15:

15. The one who defrauds by means of use of a purchase, credit or debit card which has been falsified, modified, thieved, robbed, lost or obtained from its legitimate holder by means of deceit or by means of non-authorized use of its data, irrespective of whether it is carried out through an automatic operation.

Venezuela, Law 37.313/2001, Sections 16 and 17:

*Fraudulent management of intelligent tags or analogous tools.* Every person who, by any means, creates, captures, records, copy, change, replicate or eliminate the data or information contained in an intelligent tag [...].

The same penalty shall apply to a person, who [...] acquires, commercializes, possesses, distribute, sell or perform any kind of intermediation of intelligent tags [...].

*Misappropriation of intelligent tags or of an instrument driven to the same purposes,* [...]

The same penalty shall apply to who acquires or receive the tag or instrument to which this section refers to.

## 20. Unauthorized use of credit card data

Canada, Bill S-4 amending the Criminal Code (identity theft and related misconduct):

Every person who, fraudulently and without colour of right, possesses, uses, traffics in or permits another person to use credit card data, including personal authentication information, whether or not the data is authentic, that would enable a person to use a credit card or to obtain the services that are provided by the issuer of a credit card to credit card holders is guilty of [...]

## 21. Identity theft

Some definitions of identity theft link it to fraud, while some others do not tie its application to the perpetration of fraud. “Theft” may be used in the sense of use, rather than in the sense of obtaining.

United States, 18 U.S.C. § 1028(a)(7), Act of Identity Theft:

Knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

Ibid., 15 U.S.C. 1681a (q)(3), Definition of Identity Theft:

Identity theft—the term “identity theft” means a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.

(a) The term “identity theft” means a fraud committed or attempted using the identifying information of another person without lawful authority.

(b) The term “identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

(1) Name, Social Security Number, date of birth, official state- or government-issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation.

(3) Unique electronic identification number, address or routing code.

(4) Telecommunication identifying information or access device.

Canada, Bill S-4 amending the Criminal Code (identity theft and related misconduct), Section 402.2:

(1) Identity theft: Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

Ibid., Section 402.1:

For the purposes of sections 402.2 and 403, "identity information" means any information—including biological or physiological information—of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's license number or password.

## 22. Computer-related identity theft

United States, 18 U.S.C. § 1030(a)(2), Fraud and related activity in connection with computers:

- 2) [Whoever] intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains:
  - (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
  - (B) information from any department or agency of the United States; or
  - (C) information from any protected computer if the conduct involved an interstate or foreign communication;

## 23. Preparation

The legal concept of preparation raises questions as to how legislation defines, or shall define, a crime and the preparatory steps associated with it.

Germany, Criminal Code,<sup>28</sup> Section 275, Preparation for Counterfeiting of Official Identification Documents:

(1) Whoever prepares a counterfeiting of official identification documents by producing, procuring for himself or another, offering for sale, storing, giving to another, or undertaking to import or export:

1. Plates, frames, type, blocks, negatives, stencils or similar equipment which by its nature is suited to the commission of the act; or
2. Paper, which is identical or confusingly similar to the type of paper which is designated for the production of official identification documents and specially protected against imitation; or
3. Blank forms for official identification documents,

shall be punished with imprisonment for not more than two years or a fine.

(2) If the perpetrator acts professionally or as a member of a gang which has combined for the continued commission of crimes under subsection (1), then the punishment shall be imprisonment from three months to five years.

(3) Section 149 subsections (2) and (3), shall apply accordingly.

Germany, Criminal Code,<sup>29</sup> Section 202c:

Preparation of the Interception of Data and Data Espionage.

(1) Whoever prepares a crime under the term of Section 202a or 202b, by producing, obtaining himself or another, selling, surrendering to another, disseminating or making available to third parties in any other way:

1. Passwords or any further protection-code, which enable the access to data (§ 202a, subsection 2), or
2. Software, whose purpose is the commission of such a crime, shall be punished with imprisonment for not more than one years or a fine.

## 24. Obtaining

There are various ways used by offenders to get possession of identity-related information, and those have been addressed in national laws.

<sup>28</sup> German Criminal Code in the version promulgated on 13 November 1998, *Federal Law Gazette [Bundesgesetzblatt]* I page 3322, last amended by Article 3 of the Law of 2 October 2009, *Federal Law Gazette* I page 3214, see: [http://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#StGBengl\\_000P169](http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169).

<sup>29</sup> *Ibid.*

United Kingdom, Identity Cards Act 2006, Section 8:

For the purposes of this section [...]; and an identity document was improperly obtained if false information was provided, in or in connection with the application for its issue or an application for its modification, to the person who issued it or (as the case may be) to a person entitled to modify it [...]

France, Criminal Code,<sup>30</sup> Article 441-6:

Unlawfully obtaining from a public administration or from an institution discharging a public service mission, by any fraudulent means, any document intended to establish a right, an identity or a capacity, or to grant an authorisation is punished by two years' imprisonment and a fine of €30,000.

The same penalties apply to the submission of a false statement so as to obtain from a public administration or from an institution discharging a public service mission an allowance, a cash payment or benefit that is not due.

France, Criminal Code,<sup>31</sup> Article 441-5:

Unlawfully procuring for another person a document delivered by a public body for the purpose of establishing a right, an identity or capacity, or the grant of an authorisation is punished by five years' imprisonment and a fine of €75,000.

The penalty is increased to seven years' imprisonment and to a fine of €100,000 where the offence is committed:

- 1) by a person holding public authority or to discharge a public service mission whilst acting in the exercise of his office;
- 2) habitually;
- 3) or with an intent to facilitate the commission of a felony or to gain impunity for the perpetrator.

## 25. Transfer

Once offender possesses the identity-related information, he/she does not necessarily use it, and may rather transfer it (including, by selling it).

Canada, Bill S-4 amending the Criminal Code (identity theft and related misconduct), Section 402.2:

- (2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for

<sup>30</sup> French Penal Code, Article 441-6, Ordinance No. 2000-916 version promulgated on 19 September 2000, Article 3, Official Journal of 22 September 2000 (came into force on 1 January 2002), see: <http://www.cyberlawdb.com/docs/france/penalcode.pdf>.

<sup>31</sup> French Penal Code, Ordinance No. 2000-916 of 19 September 2000, Article 3, Official Journal of 22 September 2000 (came into force on 1 January 2002), see: <http://www.cyberlawdb.com/docs/france/penalcode.pdf>.

any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

## 26. Use

At the end of the chain of actions, the offender uses the identity-related information for the commission of other offences.

Canada, Bill S-4 amending the Criminal Code (identity theft and related misconduct), Section 402.2:

(3) For the purposes of subsections (1) and (2), an indictable offence referred to in either of those subsections includes an offence under any of the following sections:

- (a) section 57 (forgery of or uttering forged passport);
- (b) section 58 (fraudulent use of certificate of citizenship);
- (c) section 130 (personating peace officer);
- (d) section 131 (perjury);
- (e) section 342 (theft, forgery, etc., of credit card);
- (f) section 362 (false pretence or false statement);
- (g) section 366 (forgery);
- (h) section 368 (use, trafficking or possession of forged document);
- (i) section 380 (fraud); and
- (j) section 403 (identity fraud).

United States, 18 USC Section 1028, Chapter 47, Fraud and False Statements:

3) A fine under this title or imprisonment for not more than 20 years, or both, if the offence is committed:

- (a) to facilitate a drug trafficking crime (as defined in section 929(a)(2));
- (b) in connection with a crime of violence (as defined in section 924(c)(3)); or
- (c) after a prior conviction under this section becomes final

A fine under this title or imprisonment for not more than 30 years, or both, if the offence is committed to facilitate an act of domestic terrorism (as defined under section 2331(5) of this title) or an act of international terrorism (as defined in section 2331(1) of this title) [...]



## 27. Possession

Although possession of documents or apparatus associated with identity-related crime is a difficult topic to legislate, as some information and devices may never come to be used for illicit activities, or may alternatively be used for legitimate purposes, some countries have taken the initiative of regulating this issue.

United Kingdom, Identity Cards Act,<sup>32</sup> Section 25:

It is an offence for a person to have in his possession or under his control, with reasonable excuse:

- (a) an identity document that is false;
- (b) an identity document that was improperly obtained;
- (c) an identity document that relates to someone else; or
- (d) any apparatus, article or material which, to his knowledge, is or has been specially designed or adapted for the making of false identity documents or to be used in the making of such documents.

France, Criminal Code,<sup>33</sup> Article 441-3:

The unlawful possession of any of the forged documents defined by Article 441-2 is punished by two years' imprisonment and a fine of €30,000.

The penalty is increased to five years' imprisonment and to a fine of €75,000 where more than one forged documents are unlawfully possessed.

## 28. Criminal misuse

Different modalities of misuse of identity-related information have been criminalized in national laws.

Germany, Criminal Code,<sup>34</sup> Sections 276 and 281:

Procuring False Official Identification Documents:

(1) Whoever:

1. undertakes to import or export; or,
2. with the intent of using it to make deception in legal relations possible, procures for himself or another, stores or gives to another

<sup>32</sup> Identity Cards Act, of 2006.

<sup>33</sup> Ordinance No. 2000-916, of 19 September 2000, Article 3, Official Journal of 22 September 2000 (came into force on 1 January 2002).

<sup>34</sup> German Criminal Code, in the version promulgated on 13 November 1998, *Federal Law Gazette [Bundesgesetzblatt]* I page 3322, last amended by Article 3 of the Law of 2 October 2009, *Federal Law Gazette I* page 3214, see: [http://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#StGBengl\\_000P169](http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P169).

a counterfeit or falsified official identification document or an official identification document which contains a false certification of the type indicated in Sections 271 and 348, shall be punished with imprisonment for not more than two years or a fine.

(2) If the perpetrator acts on a commercial basis or as a member of a gang, which has combined for the continued commission of crimes under subsection (1), then the punishment shall be imprisonment from three months to five years.

Misuse of identification papers:

(1) Whoever, for the purpose of deception in legal relations, uses an identification paper which was issued to another, or whoever, for the purpose of deception in legal relations, gives another an identification paper that was not issued to that person, shall be punished with imprisonment for not more than one year or a fine. An attempt shall be punishable.

(2) Certificates and other documents which are used as identification documents in transactions shall be equivalent to an identification paper.

Sweden, Criminal Code,<sup>35</sup> Section 12:

A person who misuses a passport, certificate or similar document issued in the name of a given individual, by representing himself or another as being that individual or imparts the document to be thus misused, or if he imparts a false document, which has come into being as a carbon copy or photographic reproduction or otherwise, as being a correct copy of a certain document, shall, if the act jeopardises proof, be sentenced for misuse of document to a fine or imprisonment for at most six months or, if the crime is gross, to imprisonment for at most two years.

## 29. Aggravating circumstances

The circumstances which may aggravate identity-related offences have also attracted the attention of legislators.

United States, 18 U.S.C. § 1028(a)(7), Aggravated identity theft:

Offenses:

(1) *In general*—Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

(2) *Terrorism offense*—Whoever, during and in relation to any felony violation enumerated in section 2332b (g)(5)(B), knowingly transfers, possesses, or uses, without

<sup>35</sup> Sweden Criminal Code, of 1965, Chapter 15, on Perjury, False Prosecution and Other Untrue Statements, Section 12, see: <http://www.cyberlawdb.com/docs/sweden/penalcode.pdf>.

lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

Chile, Criminal Code,<sup>36</sup> Section 269H, Circumstances of punitive aggravation:

The penalties to be imposed as per the sections included in this Title shall be increased by fifty per cent or by seventy-five per cent when the conduct is perpetrated:

1. Over computer networks or systems or of state communications or of the financial system, national or foreign.
2. By public employee in the exercise of his functions.
3. Benefitting from the trust deposited by the owner of the information or by the one who has contractual relationship with the latter.
4. Revealing or letting know the contents of information to unfavor another party.
5. Obtaining benefit for himself or for a third party.
6. With terrorist purposes or generating risk for the national security or defense.
7. Using a third party of good faith as instrument.
8. If the one who incurs in those conducts is the person in charge of the management, administration or control of such information [...].

France, Criminal Code, Section 441-2:<sup>37</sup>

The penalty is increased to seven years' imprisonment and to a fine of €100,000 where the forgery or the use of the forgery is perpetrated:

1. by a person holding public authority or discharging a public service mission acting in the exercise of his office;
2. habitually;
3. or with the intent to facilitate the commission of a felony or to gain impunity for the perpetrator.

## 30. Fraud/identity fraud

Legislators have also addressed identity-related information in connection with fraud in general or established ad hoc identity fraud offences.

<sup>36</sup> Chilean Penal Code, of 12 November 1874, see: <http://www.servicioweb.cl/juridico/Codigo%20Penal%20de%20Chile%20libro2.htm>.

<sup>37</sup> French Criminal Code, Act No. 1996-647, of 22 July 1996, Article 2, Official Journal of 23 July 1996, see: <http://www.cyberlawdb.com/docs/france/penalcode.pdf>.

Canada, Bill S-4 amending the Criminal Code (identity theft and related misconduct), Section 403 (Identity fraud):

- (1) Everyone commits an offence who fraudulently personates another person, living or dead,
  - (a) with intent to gain advantage for themselves or another person;
  - (b) with intent to obtain any property or an interest in any property;
  - (c) with intent to cause disadvantage to the person being personated or another person; or
  - (d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.

## 31. Intent to commit another offence

Some researched countries possess legislation establishing a link between identity-related crime and the intent to perpetrate other crimes.

United Kingdom, Identity Cards Act,<sup>38</sup> Sections 1 to 4:

- (1) It is an offence for a person with the requisite intention to have in his possession or under his control:
  - (a) an identity document that is false and that he knows or believes to be false;
  - (b) an identity document that was improperly obtained and that he knows or believes to have been improperly obtained; or
  - (c) an identity document that relates to someone else.
- (2) The requisite intention for the purposes of subsection (1) is:
  - (a) the intention of using the document for establishing registrable facts about himself; or
  - (b) the intention of allowing or inducing another to use it for establishing, ascertaining or verifying registrable facts about himself or about any other person (with the exception, in the case of a document within paragraph (c) of that subsection, of the individual to whom it relates).
- (3) It is an offence for a person with the requisite intention to make, or to have in his possession or under his control:
  - (a) any apparatus which, to his knowledge, is or has been specially designed or adapted for the making of false identity documents; or

<sup>38</sup> Identity Cards Act, of 2006.

- (b) any article or material which, to his knowledge, is or has been specially designed or adapted to be used in the making of false identity documents.
- (4) The requisite intention for the purposes of subsection (3) is:
  - (a) that he or another will make a false identity document; and
  - (b) that the document will be used by somebody for establishing, ascertaining or verifying registrable facts about a person.

Nigeria, Criminal Code,<sup>39</sup> Section 479:

Any person who knowingly and with an intent to procure the same to be inserted in a register of births, deaths, or marriages, makes any false statement touching any matter required by law to be registered in any such register, is guilty of a felony, and is liable to imprisonment for three years.

---

<sup>39</sup> Nigerian Criminal Code, of 1990, Chapter 18, see: <http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm>.

# ANNEXES

## A.1. Identity-related crime legislation: definitions, means or format of identity-related information, protected ID information

Country	Legislation	Identity-related information concept			
		Denomination	Form of information	Social Security no./ single personal identification no./ health insurance no.	Name/address/ date of birth/ written signature
ALBANIA	Criminal Code	Identity documents	Any	Yes	Yes
ARGENTINA	Criminal Code	Personal database	Databases, data files	Yes	Yes
AUSTRALIA	Privacy Act (1988)	Personal information	Any—information or opinion		
AUSTRIA	Criminal Code, and Law 565/78	Personal data	Any	Yes	
AZERBAIJAN	Criminal Code	Law protected computer info.	Computers, systems, networks		
BOLIVIA (Plurinational State of)	Law 1768/97	Computer data	Electronic support		
BRAZIL	Criminal Code	-	Documental		
BULGARIA	Criminal Code	Personal data, passwords	Any		
CANADA	Bill S-4	-	Any (including biological/ physiological)	Yes	Yes
CHILE	Law 19.223/93	System data	Data contained in a system	Yes	
CHINA	Criminal Code	Citizen's identification cards	Any		
COLOMBIA	Criminal Code	Personal data	Databases		
COSTA RICA	Law 8148	Secrets	Electronic media		



**Identity-related information categories**

	Birth, marital status or death certificate/ ID card/passport/ immigration doc.	Driving license/ military status card/ voter card for political elections	Credit or debit card no./financial institution account no.	E-mail login/e-mail or web browsing passwords/Mac-address or IP-address/electronic or digital signature/user name	Fingerprint/ voice print/retina image/iris image/ DNA profile
	Yes				
	Yes	Yes			
	Yes	Yes	Yes	Yes	Yes

Country	Legislation	Identity-related information concept			Social Security no./ single personal identification no./ health insurance no.	Name/address/ date of birth/ written signature	
		Denomination	Form of information				
<b>ECUADOR</b>	Criminal Code (amended in 2002)	Personal doc., restricted personal or family data	Data and electronic media				
<b>ESTONIA</b>	Criminal Code	Personal information of delicate character	Computers, data banks				
<b>FRANCE</b>	Criminal Code, and Law 88-19/88	Data	Any				
<b>GEORGIA</b>	Criminal Code	Law protected computer information	Computers, systems, networks				
<b>GERMANY</b>	Criminal Code	Identification paper	Documental				
<b>HUNGARY</b>	Act LXIII of 1992	Personal data	Any				
<b>INDIA</b>	Information technology Act (2008)	Identity information	Any				
<b>ITALY</b>	Criminal Code	Computer systems relating to public order	Code, key words	Yes			
<b>JAPAN</b>	Criminal Code, and Law 128/99	Electromagnetic records, Identification code	Electromagnetic				
<b>KAZAKHSTAN</b>	Criminal Code	Law protected computer information	Computers, systems, networks				
<b>KYRGYZSTAN</b>	Criminal Code	Law protected computer information	Computers, systems, networks				
<b>MEXICO</b>	Criminal Code (amended in 1999)	Information contained in systems of financial institutions	Data				
<b>NIGERIA</b>	Criminal code	Electronic documents	Any				
<b>PERU</b>	Criminal Code	Undue access to database	Database or system				
<b>PHILIPPINES</b>	Access Devices Regulation Act of 1998	Identities, PIN number	Card, plate, code, equipment				





Country	Legislation	Identity-related information concept			
		Denomination	Form of information	Social Security no./ single personal identification no./ health insurance no.	Name/address/ date of birth/ written signature
PORTUGAL	Law 109/91	Confidential data			
REPUBLIC OF MOLDOVA	Law No. 17-XVI/ 2007	Personal data	Information systems, biometrical		
ROMANIA	Anti Corruption Law of	Data on the users			
RUSSIAN FEDERATION	Federal Law No.152-FZ/2006 (Law on Personal Data)	Personal data, identity data	Databases, information systems, biometrical,		
SOUTH AFRICA	ECT Act	Personal information	Any	Yes	Yes
SPAIN	Criminal Code— Law 10/1995	Data of personal character	Computer, electronic or telematic files and media	Yes	
SWITZERLAND	Criminal Code				
SWEDEN	Criminal Code	Data	False mark		
TURKEY	Criminal Code	Counterfeit or falsified bank or credit card	Bank or credit card		
UNITED KINGDOM	UK Fraud Act/ UK Identity Cards Act		Documental		
UNITED STATES	US Code—Title 18, Chapter 47			Yes	
VENEZUELA	Law 37.313/2001	Personal or patrimonial data or information	Data		

## Identity-related information categories

Birth, marital status or death certificate/ ID card/passport/ immigration doc.	Driving license/ military status card/ voter card for political elections	Credit or debit card no./financial institution account no.	E-mail login/e-mail or web browsing passwords/Mac-address or IP-address/electronic or digital signature/user name	Fingerprint/ voice print/retina image/iris image/ DNA profile
Yes	Yes	Yes		Yes
Yes	Yes	Yes		
Yes	Yes	Yes	Yes	

## A.2. Identity-related crime typologies and categories of conducts

Country	Legislation	Production of a counterfeit document or falsification of a genuine document	Individual unlawful use of identity-related information	
		Produce/alter/interfere/ authenticate/assemble/make/ adapt/modify	Possess/use/hold/obtain/ control/give or present false information/access (including breaking through access-protection)/procure/assign	Omit/suppress
ALBANIA	Criminal Code	Yes	Yes	
ARGENTINA	Penal Code	Yes	Yes	
BRAZIL	Criminal Code	Yes	Yes	Yes
CANADA	Bill S-4		Yes	
GERMANY	German Criminal Code	Yes	Yes	Yes
INDIA	IT Act (2008)		Yes	
JAPAN	Law 128, of 1999	Yes	Yes	
SOUTH AFRICA	ECT Act	Yes	Yes	
UNITED KINGDOM	UK Fraud Act/ UK Identity Cards Act	Yes	Yes	
UNITED STATES	US Code	Yes	Yes	

## A.3. Identity-related crime typologies: subjective elements and requirements

Country	Legislation	Intent				
		To commit/aid/ abet any unlawful activity	To defraud	To deceive	To obtain for himself or a third person an unlawful material benefit/advantage	To use the document for establishing registrable facts about oneself
ALBANIA	Criminal Code					
ARGENTINA	Penal Code	Yes	Yes	Yes		
AUSTRALIA	Privacy Act (1988)					
BRAZIL	Criminal Code		Yes	Yes	Yes	
CANADA	Bill S-4	Yes	Yes	Yes	Yes	
GERMANY	German Criminal Code	Yes	Yes	Yes	Yes	
INDIA	IT Act 2008		Yes	Yes		
JAPAN	Law 128, of 1999			Yes		
SOUTH AFRICA	ECT Act	Yes		Yes	Yes	
UNITED KINGDOM	UK Fraud Act/ UK Identity Cards Act		Yes			Yes
UNITED STATES	US Code	Yes	Yes	Yes		

	Collective unlawful use of Identity-related information	Traffic of Identity-related information	Damage to another's Identity-related information	Attempt/ conspiracy/ aid/abet
	Transfer/make available placing online/transmit/distribute/sell or supply/offer for sale or to supply (or possess for such purposes)/surrender/disseminate	Transfer/transport/dispose (or make/obtain control with such intent)/store/undertaking to import or export	Provoking or affirming a mistake/pretending that false facts exist/destroying, occulting distorting or suppressing true facts/influencing the result of a data processing operation	
	Yes			
	Yes	Yes		
	Yes		Yes	
	Yes	Yes		
	Yes	Yes	Yes	Yes
	Yes			Yes
	Yes		Yes	Yes
	Yes			
	Yes	Yes		Yes

	Lack of authorization or permission	Awareness belief or recklessness		
		As to obtaining or possessing someone else's identity info.	As to the falseness or improper obtainance of the document	As to whether the information will be used to commit an indictable offence
		Yes		Yes
	Yes			
	Yes			
			Yes	Yes
	Yes			

### Samples of national laws, and relevant sources

Country	Legislation	Source
<b>ALBANIA</b>	Criminal Code, and Law No. 7895, of 27 January 1995	<a href="http://www.cyberlawdb.com/docs/albania/albania.pdf">http://www.cyberlawdb.com/docs/albania/albania.pdf</a>
<b>ARMENIA</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/armenia/armenia.pdf">http://www.cyberlawdb.com/docs/armenia/armenia.pdf</a>
<b>ARGENTINA</b>	Criminal code, and Law No. 25.286/2008	<a href="http://www.cyberlawdb.com/docs/argentina/argentina.pdf">http://www.cyberlawdb.com/docs/argentina/argentina.pdf</a>
<b>AUSTRALIA</b>	Privacy Act, 1988	<a href="http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/CDFBC6BC359968E4CA257758001791A7?OpenDocument">http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/CDFBC6BC359968E4CA257758001791A7?OpenDocument</a>
<b>AUSTRIA</b>	Criminal Code, and Federal Act Concerning the Protection of Personal Data	<a href="http://www.dsk.gv.at/site/6230/default.aspx#E15">http://www.dsk.gv.at/site/6230/default.aspx#E15</a> <a href="http://www.cyberlawdb.com/docs/austria/austria.pdf">http://www.cyberlawdb.com/docs/austria/austria.pdf</a>
<b>AZERBAIJAN</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>BARBADOS</b>	Computer Misuse Act, of 18 July 2005	<a href="http://www.cyberlawdb.com/docs/barbados/computer_misuse.pdf">http://www.cyberlawdb.com/docs/barbados/computer_misuse.pdf</a>
<b>BELARUS</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>BOLIVIA (Plurinational State of)</b>	Criminal Code	<a href="http://www.oas.org/juridico/spanish/gapeca_sp_docs_bol1.pdf">http://www.oas.org/juridico/spanish/gapeca_sp_docs_bol1.pdf</a>
<b>BOTSWANA</b>	Criminal Code	<a href="http://www.laws.gov.bw/">http://www.laws.gov.bw/</a>
<b>BRAZIL</b>	Criminal Code	<a href="http://www.amperj.org.br/store/legislacao/codigos/cp_DL2848.pdf">http://www.amperj.org.br/store/legislacao/codigos/cp_DL2848.pdf</a>
<b>BULGARIA</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/bulgaria/bulgaria.pdf">http://www.cyberlawdb.com/docs/bulgaria/bulgaria.pdf</a>
<b>CANADA</b>	Bill S-4, 2009	<a href="http://www2.parl.gc.ca/content/hoc/Bills/402/Government/S-4/S-4_4/S-4_4.PDF">http://www2.parl.gc.ca/content/hoc/Bills/402/Government/S-4/S-4_4/S-4_4.PDF</a>
<b>CHILE</b>	Law No. 19223	<a href="http://www.leychile.cl/Navegar?idNorma=30590&amp;buscar=19.223">http://www.leychile.cl/Navegar?idNorma=30590&amp;buscar=19.223</a>
<b>CHINA</b>	Criminal Code	<a href="http://www.colaw.cn/findlaw/crime/criminallaw3.html">http://www.colaw.cn/findlaw/crime/criminallaw3.html</a>
<b>COLOMBIA</b>	Criminal Code and Law No. 1273/2009	<a href="http://www.derechos.org/nizkor/colombia/doc/penal.html">http://www.derechos.org/nizkor/colombia/doc/penal.html</a> <a href="http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html">http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html</a>
<b>COSTA RICA</b>	Law No. 4573	<a href="http://www.pgr.go.cr/scij/scripts/TextoCompleto.dll?Texto&amp;nNorma=47430&amp;nVersion=50318&amp;nTamanoLetra=10&amp;strWebNormativa=http://www.pgr.go.cr/scij/&amp;strODBC=DSN=SCIJ_NRM;UID=sa;PWD=scij;DATABASE=SCIJ_NRM;&amp;strServidor=\\pgr04&amp;strUnidad=D:&amp;strJavaScript=NO">http://www.pgr.go.cr/scij/scripts/TextoCompleto.dll?Texto&amp;nNorma=47430&amp;nVersion=50318&amp;nTamanoLetra=10&amp;strWebNormativa=http://www.pgr.go.cr/scij/&amp;strODBC=DSN=SCIJ_NRM;UID=sa;PWD=scij;DATABASE=SCIJ_NRM;&amp;strServidor=\\pgr04&amp;strUnidad=D:&amp;strJavaScript=NO</a>
<b>CROATIA</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/croatia/croatia.pdf">http://www.cyberlawdb.com/docs/croatia/croatia.pdf</a>
<b>CYPRUS</b>	Law No. 22(III)04	<a href="http://www.cyberlawdb.com/docs/cyprus/cyprus.pdf">http://www.cyberlawdb.com/docs/cyprus/cyprus.pdf</a>
<b>CZECH REPUBLIC</b>	Criminal Code, and Criminal Procedure Code	<a href="http://www.cyberlawdb.com/docs/czech/czech.pdf">http://www.cyberlawdb.com/docs/czech/czech.pdf</a>
<b>ECUADOR</b>	Criminal Code	<a href="http://www.miliarium.com/Paginas/Leyes/Internacional/Ecuador/General/cp.pdf">http://www.miliarium.com/Paginas/Leyes/Internacional/Ecuador/General/cp.pdf</a>
<b>ESTONIA</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>FRANCE</b>	Criminal Code, and Law No. 88-19/88	<a href="http://www.crime-research.org/articles/cybercrime-in-france-overview/2">http://www.crime-research.org/articles/cybercrime-in-france-overview/2</a>
<b>GERMANY</b>	Federal Data Protection Act	<a href="http://www.bdd.de/Download/bdsg_eng.pdf">http://www.bdd.de/Download/bdsg_eng.pdf</a>

Country	Legislation	Source
<b>GEORGIA</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>HUNGARY</b>	Act No. LXIII of 1992	<a href="http://abiweb.obh.hu/adatved/indexek/AVTV-EN.htm">http://abiweb.obh.hu/adatved/indexek/AVTV-EN.htm</a>
<b>INDIA</b>	The Information Technology Act, 2008	<a href="http://cybercrime.planetindia.net/it-act-2008.htm">http://cybercrime.planetindia.net/it-act-2008.htm</a>
<b>ISRAEL</b>	The Computers Law of 1995	<a href="http://www.cybercrimelaw.net/Israel.html">http://www.cybercrimelaw.net/Israel.html</a>
<b>ITALY</b>	Criminal Code	<a href="http://it.wikisource.org/wiki/Codice_penale/Libro_II">http://it.wikisource.org/wiki/Codice_penale/Libro_II</a> <a href="http://guide.supereva.it/diritto/interventi/2001/04/39144.shtml">http://guide.supereva.it/diritto/interventi/2001/04/39144.shtml</a> <a href="http://www.cyberlawdb.com/docs/italy/italy.pdf">http://www.cyberlawdb.com/docs/italy/italy.pdf</a>
<b>INDONESIA</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/indonesia/indonesia.pdf">http://www.cyberlawdb.com/docs/indonesia/indonesia.pdf</a>
<b>IRELAND</b>	Criminal Justice Act, 2001	<a href="http://www.irishstatutebook.ie/2001/en/act/pub/0050/print.html">http://www.irishstatutebook.ie/2001/en/act/pub/0050/print.html</a>
<b>JAMAICA</b>	The Interception of Communications Act	<a href="http://www.cyberlawdb.com/docs/jamaica/intercep_commun.pdf">http://www.cyberlawdb.com/docs/jamaica/intercep_commun.pdf</a>
<b>JAPAN</b>	Criminal Code, and Law No. 128/99	<a href="http://www.npa.go.jp/english/kokusai9/White_Paper_2009_4.pdf">http://www.npa.go.jp/english/kokusai9/White_Paper_2009_4.pdf</a>
<b>KAZA-KHSTAN</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>KYR-GYZSTAN</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>LITHUANIA</b>	Criminal Code, and Criminal Procedures Code	<a href="http://www.cyberlawdb.com/docs/lithuania/lithuania.pdf">http://www.cyberlawdb.com/docs/lithuania/lithuania.pdf</a>
<b>MALAYSIA</b>	Computer Crimes Act of 1997	<a href="http://www.cyberlawdb.com/docs/malaysia/cc.pdf">http://www.cyberlawdb.com/docs/malaysia/cc.pdf</a>
<b>MEXICO</b>	Criminal Code	<a href="http://www.delitosinformaticos.com/delitos/ensayomexico.shtml">http://www.delitosinformaticos.com/delitos/ensayomexico.shtml</a>
<b>NIGERIA</b>	Criminal Code	<a href="http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm#Chapter18">http://www.nigeria-law.org/Criminal%20Code%20Act-PartIII-IV.htm#Chapter18</a>
<b>PERU</b>	Criminal Code	<a href="http://www.policiainformatica.gob.pe/pdf/ley27309.pdf">http://www.policiainformatica.gob.pe/pdf/ley27309.pdf</a>
<b>PORTUGAL</b>	Criminal Code	<a href="http://bdjur.almedina.net/citem.php?field=node_id&amp;value=1224791">http://bdjur.almedina.net/citem.php?field=node_id&amp;value=1224791</a>
<b>PHILIPPINES</b>	Phillipines Electronic Commerce Act	<a href="http://www.cyberlawdb.com/docs/philippines/philippines.pdf">http://www.cyberlawdb.com/docs/philippines/philippines.pdf</a>
<b>REPUBLIC OF MOLDOVA</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/moldova/moldova.pdf">http://www.cyberlawdb.com/docs/moldova/moldova.pdf</a>
<b>ROMANIA</b>	Anti-Corruption Law	<a href="http://www.crime-research.org/library/Romania.html">http://www.crime-research.org/library/Romania.html</a>
<b>RUSSIAN FEDERATION</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>SAUDI ARABIA</b>	Anti-Cyber Crime Law no. 11428/26 March 2007	<a href="http://www.saudiembassy.net/announcement/announcement03260701.aspx">http://www.saudiembassy.net/announcement/announcement03260701.aspx</a>
<b>SINGAPORE</b>	Computer Misuse Act	<a href="http://www.cyberlawdb.com/docs/singapore/cma.pdf">http://www.cyberlawdb.com/docs/singapore/cma.pdf</a>
<b>SLOVAKIA</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/slovakia/slovakia.pdf">http://www.cyberlawdb.com/docs/slovakia/slovakia.pdf</a>
<b>SOUTH AFRICA</b>	ECT Act of 2002	<a href="http://www.internet.org.za/ect_act.html">http://www.internet.org.za/ect_act.html</a>

Country	Legislation	Source
<b>SPAIN</b>	Criminal Code	<a href="http://www.delitosinformaticos.com/legislacion/espana.shtml">http://www.delitosinformaticos.com/legislacion/espana.shtml</a>
<b>SWEDEN</b>	Personal Data Act	<a href="http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf">http://www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf</a>
<b>SWITZERLAND</b>	Criminal Code	<a href="http://www.rhf.admin.ch/rhf/it/home/straf/recht/multilateral/ccc.html">http://www.rhf.admin.ch/rhf/it/home/straf/recht/multilateral/ccc.html</a>
<b>TAJIKISTAN</b>	Criminal Code	<a href="http://www.crime-research.org/library/Romania.html">http://www.crime-research.org/library/Romania.html</a>
<b>THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/macedonia/macedonia.pdf">http://www.cyberlawdb.com/docs/macedonia/macedonia.pdf</a>
<b>TURKEY</b>	Criminal Code	<a href="http://www.cyberlawdb.com/docs/turkey/turkey.pdf">http://www.cyberlawdb.com/docs/turkey/turkey.pdf</a>
<b>UKRAINE</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>UNITED ARAB EMIRATES</b>	Federal Law No. (2), of 2006	<a href="http://www.aecert.ae/Prevention_of_Information_Technology_Crimes_English.pdf">http://www.aecert.ae/Prevention_of_Information_Technology_Crimes_English.pdf</a>
<b>UNITED KINGDOM</b>	Fraud Act of 2006, and Identity Card Act of 2006	<a href="http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf">http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf</a> <a href="http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf">http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf</a> .
<b>UNITED STATES OF AMERICA</b>	Criminal Code	<a href="http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_l_20_47.html">http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_l_20_47.html</a>
<b>UZBEKISTAN</b>	Criminal Code	<a href="http://www.crime-research.org/library/Criminal_Codes.html">http://www.crime-research.org/library/Criminal_Codes.html</a>
<b>VENEZUELA</b>	Law No. 37.313/2001	<a href="http://fundabit.me.gob.ve/documento/LECDI.pdf">http://fundabit.me.gob.ve/documento/LECDI.pdf</a>
<b>ZAMBIA</b>	Computer Misuse and Crimes Law	<a href="http://www.parliament.gov.zm/index.php?option=com_docman&amp;task=doc_view&amp;gid=112">http://www.parliament.gov.zm/index.php?option=com_docman&amp;task=doc_view&amp;gid=112</a>



# BIBLIOGRAPHY

1. *Aboso, Gustavo Eduardo, and Zapata, Maria Florência*, “Cibercriminalidad y Derecho Penal”, Montevideo, Bef, 2006, pages 79-82.
2. Cahiers de la Sécurité, No. 6, Institut National des Hautes Études de Sécurité, oct-déc. 2008, pages 42-48.
3. *Cifuentes, Santos*, “Derechos Personalísimos”, Buenos Aires, Astrea, 2008, pages 703-711.
4. *Cruz, Danielle da Rocha Cruz*, “Criminalidade informática—tipificação penal das condutas ilícitas realizadas com cartões de crédito”, Rio de Janeiro, Forense, 2006, pages 84-89, 190-200.
5. *Desgens-Pasanau, Guillaume*, “L’identité à l’ère numérique”, Paris, Dalloz, 2009, pages 98-105, 117-119.
6. “Essential Elements of Criminal Laws to Address Identity-Related Crime”, February 2009, circulated by the G8 Lyon-Roma Anti-Crime and Terrorism Group Criminal and Legal Affairs Subgroup.
7. *Faggioli, Gabriele*, “Computer Crimes”, Napoli, Esselibri, 2002, pages 25, 28.
8. *Feliciano, Guilherme Guimarães*, “Informática e Criminalidade”, Ribeirão Preto, Nacional de Direito, 2001, pages 94, 111.
9. *Fillia, Leonardo César, et al*, “Análisis Integrado de la Criminalidad Informática”, Buenos Aires, Fabián J. Di Plácido, 2007, pages 71-74, 182-195.
10. *Gil, Antonio de Loureiro*, “Fraudes informatizadas”, São Paulo, Atlas, 1996, pages 192.
11. *Godart, Didier*, “Sécurité Informatique—risques, strategies et solutions”, Liège, CCI, 2005, page 95
12. “Internet et la société de contrôle: le piège?”, Cités, Paris, Presses Universitaires de France, 2009, page 11.
13. *Iteanu, Olivier*, “L’identité numérique en question”, Paris, Eyrolles, 2008, pages 137-149.
14. *Jaber, Abbas*, “Les infractions commises sur Internet”, Paris, L’Harmattan, 2009, pages 34-35, 59-62.
15. *Leiva, Renato Javier Fijena*, “Chile, la Protección Penal de la Intimidación y el Delito Informático”, Santiago, Editorial Jurídica de Chile, 1992, pages 56-69.
16. *Palazzi, Pablo A.*, “Los Delitos Informáticos en el Código Penal”, Buenos Aires, Abeledo-Perrot, 2009, pages 130.
17. *Pouillet, Yves*, “Derecho a la intimidad y a la protección de datos personales”, Buenos Aires, Heliasta, 2009, pages 113-138.
18. *Quémener, Myriam, and Ferry, Joël*, “Cybercriminalité—défi mondial et réponses”, Paris, Economica, 2007, pages 106.

19. *Riquert, Marcelo A.*, “Delincuencia Informática em Argentina y el Mercosur”, Buenos Aires, Ediar, 2009, pages 122, 139-140.
20. *Riquert, Marcelo A.*, “Informática y Derecho Penal Argentino”, Buenos Aires, AdHoc, 1999, pages 41.
21. *Rodríguez, José Julio Fernández*, “Secreto e intervención de las comunicaciones en Internet”, Madrid, Civitas, 2004, pages 71, 168-169.
22. *Rosende, Eduardo E.*, “Derecho Penal e Informatica—Especial referencia a las amenazas lógico informáticas”, Buenos Aires, Fabián J. Di Plácido, 2008, pages 218-274.
23. *Sarzana, Carlo*, “Informatica e Diritto Penale”, Milano, Giuffrè, 1994, pages 69, 247-463.
24. *Shalhoub, Zeinab Karake*, and *Al Qasimi, Sheikha Lubna*, “Cyber Law and Cyber Security in Developing and Emerging Economies”, Cheltenham, Elgar, 2010, pages 175-184.
25. *Suarez, José María Álvarez-Cienfuegos*, “La defensa de la intimidad de los ciudadanos y la tecnología informática”, Pamplona, Aranzadi, 1999, page 81.
26. *Sueiro, Carlos, et al.*, “Análisis integrado de la criminalidad informática”, Buenos Aires, Fabián J. di Plácido, 2007, pages 71-72, 183-195.
27. *Ucich, Rodolfo D.*, “El derecho a la intimidad en Internet y en las comunicaciones electrónicas”, Buenos Aires, AdHoc, 2009, pages 81-90.
28. United Nations Convention Against International Organized Crime and the Protocols thereto, Sections 2, 3, and 31.
29. *Vianna, Julio Lima*, “Fundamentos de Direito Penal Informático—do acesso não autorizado a sistemas computacionais”, Rio de Janeiro, Forense, 2003, pages 35-44.
30. *Vieira, Jair Lot*, “Crimes na Internet, interpretados pelos tribunais—repertório de jurisprudência e legislação”, Bauru, Edipro, 2009, pages 123-124.
31. *Vieira, Tatiana Malta*, “O direito à privacidade na sociedade da informação”, Porto Alegre, Fabris, 2007, pages 267-274.
32. *Zaniolo, Pedro Augusto*, “Crimes Modernos—o impacto da tecnologia no Direito”, Curitiba, Juruá, 2007, pages 161-163, 235-236.







# IDENTITY-RELATED CRIME VICTIM ISSUES: A DISCUSSION PAPER\*

**Philippa Lawson**

**Associate, International Centre for Criminal Law Reform  
and Criminal Justice Policy, Canada**

---

\*The present discussion paper was prepared for use as working document at the third meeting of the Core Group of Experts on Identity-Related Crime, held in Vienna, Austria, on 20-22 January 2009. It was also submitted as a Conference Room Paper to the Commission on Crime Prevention and Criminal Justice at its eighteenth session, held in Vienna on 16-24 April 2009 (E/CN.15/2009/CRP.14). The opinions expressed in this paper are those of the author and do not reflect the views of the United Nations.



# Contents

	<i>Page</i>
I. Introduction .....	111
1. Terminology.....	111
II. RANGE AND TYPES OF IDENTITY-RELATED CRIME VICTIMS .....	113
1. Range of identity-related crime victims .....	113
2. Victim typologies.....	116
III. LEGAL BASES FOR RESTORATION OF VICTIM IDENTITY .....	129
1. Normative basis for victim remediation: victims' rights initiatives.....	129
2. Legal basis for restoration: criminal law .....	132
3. Legal basis for restoration: civil law .....	133
4. Relevant human rights .....	141
5. Legal framework for international cooperation in assisting victims of crime .....	148
IV. INVENTORY OF PRACTICES FOR VICTIM REMEDIATION .....	149
1. Public sector practices .....	149
2. Private sector practices.....	161







# I. INTRODUCTION

This discussion paper was commissioned by the United Nations Office on Drugs and Crime (“UNODC”) further to its 2004 study on “Fraud and the criminal misuse and falsification of identity” and its mandates arising from ECOSOC resolutions 2004/26 and 2007/20. Its purpose is to assist the UNODC in developing strategies and practical action for combating identity-related crime, improving communication between crime experts and victim experts, and identifying areas in need of further research regarding this form of crime. The discussion paper covers the following issues:

- (a) The range and types of victims of identity-related crime;
- (b) Legal bases for victim remediation, including an analysis of rights to identity, reputation and privacy; and
- (c) An inventory of state and private sector practices for victim support and remediation.

## 1. Terminology


Consistent with the report of the Secretary-General on the results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity,<sup>1</sup> “identity-related crime” in this paper refers to all forms of wrongdoing conducted under the guise of another person’s identity, as well as to preparatory acts involving the collection, manipulation and trading of identity information. It includes acts that may not be legally recognized as crimes. Most of these acts can be considered either “identity theft” or “identity fraud”, the former referring to the misappropriation of genuine identity information or documents, and the latter referring to the use of identity information to deceive others. Some acts, such as trafficking in personal data, are neither “theft” nor “fraud”.

The terms “thief”, “fraudster”, and “criminal” are used in this paper to refer to the individual wrongdoer, regardless of whether he or she committed a recognized crime.

The term “rights” is used broadly to refer to human rights as set out in international and regional instruments, domestic constitutions and human rights laws, as well as to legal rights arising from statutory obligations or common law doctrines.

<sup>1</sup> E/CN.15/2007/8.





## II. RANGE AND TYPES OF IDENTITY-RELATED CRIME VICTIMS

### 1. Range of identity-related crime victims

Identity-related crime leaves a wide range of victims in its wake, including individuals, corporations, and governments.

Such crimes typically involve the impersonation of another individual in order to obtain some kind of advantage or to avoid detection. *Individuals* are thus the primary victims of identity-related crime to the extent that it is their identities, and therefore reputations, that are corrupted or misused.

*Businesses and other private entities* are victimized when their corporate identities are misappropriated and used for unauthorized and fraudulent purposes.<sup>2</sup> Such corporate identity fraud may be used to lure individual victims into providing personal data (e.g., via phishing) or to obtain the proceeds from fraudulent real estate or corporate transactions. Other non-incorporated entities may similarly face misappropriation of their identities and suffer consequent financial and/or reputational damage.

Private organizations also suffer financially when they are defrauded by identity criminals. Such losses may be passed on in whole or in part to consumers through higher rates.

*Governments* are victimized when their services and benefits are accessed fraudulently by identity criminals. The costs of such fraud are ultimately carried by taxpayers.

This paper focuses for the most part on individual victims.

#### *Extent of individual victimization*

Statistics on the incidence of identity-related crime are poor outside the United States, and even there, they are indicative at best, reflecting only recent acknowledgement of the value in collecting such data as well as difficulties involved in collecting them. According to a leading United States survey, 5 per cent of Americans were victims of identity-related crime in 2006, an over 50 per cent increase since 2003.<sup>3</sup> In Canada, one 2008 survey found that “about 1 in 10 Canadians reports having been a victim of identity theft”,<sup>4</sup> while

<sup>2</sup>This paper does not address corporate identity theft other than briefly under the “Nature of Damages” typology of victims, and in the discussion of victim redress under civil law (“Intellectual Property”), below.

<sup>3</sup>Gartner Inc., Press Release (6 March 2007).

<sup>4</sup>EKOS Research Associates, quoted in Criminal Intelligence Service Canada, *Annual Report 2008*, “Feature Focus: Identity Theft and Identity Fraud in Canada”.

another 2008 survey found that 6.5 per cent of Canadian adults had been the victim of some kind of identity fraud in the previous year, and that very few cases were reported to the police, credit reporting agencies, or the Canadian fraud reporting agency.<sup>5</sup> A recent study in the United Kingdom found a 66 per cent increase in identity fraud victims contacting the national credit reporting agency in 2007 versus 2006,<sup>6</sup> and an almost 50 per cent increase in the first half of 2008 over the same period in 2007.<sup>7</sup> The United Kingdom financial industry also reported high rates of growth of economic identity fraud—over 200 per cent for account takeovers—in 2008.<sup>8</sup>

Despite sometimes wide divergences, statistics thus strongly suggest that the incidence of identity-related crime worldwide and the damages caused by it to all three categories of victims are growing.

### *Geographic range*

Geographically, reported identity-related crime appears to be most rampant in the United States and other English-speaking countries, but is an increasing concern in European jurisdictions.<sup>9</sup> The availability and extent of mechanisms and services designed to assist victims of identity-related crime reflects this apparent reality, with vastly more available to victims in the United States than in any other country. It is possible, however, that this apparent disparity in victimization merely reflects differences in the recognition and reporting of identity-related crime among jurisdictions.

### *Demographic range*

Individual victims of identity-related crime range across all demographics including age, gender, income, education, and ethnicity; there is no single profile of a typical victim, although certain types and/or locations of identity fraud focus on particular vulnerable groups.<sup>10</sup>

For example, children appear to be particular targets for fraud involving social security numbers or other identifying data that is unlikely to be quickly detected. This is the case, for example, with employment fraud by illegal immigrants in southern United States.<sup>11</sup> A recent study by Javelin Research in the United States found that children are at risk of identity theft, no matter the age. One child in the study had seven identities listed under their SSN, with several thousand dollars in medical bills, apartment rentals, and credit accounts in collections; another child's SSN was associated with over \$325,000 in debt.

<sup>5</sup> *Sproule and Archer*, Measuring Identity Theft in Canada: 2008 Consumer Survey, MeRC Working Paper No. 23 (July 2008) ["Sproule and Archer"].

<sup>6</sup> Experian UK, News Release (28 May 2008); see also "Privacy Watchdog concerned over surge in identity fraud", *The Press and Journal* (16 June 2008).

<sup>7</sup> Experian UK, News Release (8 October 2008).

<sup>8</sup> CIFAS, Press Release: "2008 Fraud Trends" (26 January 2009).

<sup>9</sup> FIDIS, "D12.7: Identity-related crime in Europe—Big Problem or Big Hype?" (9 June 2008) ["FIDIS"], page 62.

<sup>10</sup> Bi-national Working Group on Cross-Border Mass Marketing Fraud (Canada-United States), *Report on Identity Theft* (October 2004).

<sup>11</sup> *Steven Malanga*, "Identity Theft in America goes Hand and Hand with Illegal Immigration", see: <http://www.usbc.org/opinion/2008/spring/identity.htm>.

In addition, a 14-year-old had a more than \$600,000 mortgage in his name and the house later went into foreclosure.<sup>12</sup>

In the United States, complaint-based statistics suggest that individuals in the 18-29 age range are most likely to be victims of identity-related crime generally, and that the rate of victimization decreases with age (unlike many other forms of fraud for which the elderly are prime targets).<sup>13</sup> Complaint-based statistics from Canada suggest that middle-aged Canadians, aged 35 to 54, are the most affected by credit or debit card fraud or theft.<sup>14</sup> A United Kingdom study found some trends regarding age and gender with respect to “plastic card fraud”: men aged 35-44 and women aged 16-24 were most likely to be victims of this type of fraud.<sup>15</sup>

Experian UK reports that *tenants* are at a particularly high risk of identity fraud, noting that “People living in rented accommodation are more likely to share mailboxes and tend to move house more frequently than homeowners. This provides fraudsters with more of an opportunity to misuse credit histories that have not been updated.”<sup>16</sup>

### *Deceased individuals*

In cases where full identities are created for the purpose of obtaining official identity documents, accessing government services and/or evading authorities, *deceased persons* provide a useful basis for the fraud since they are unable to detect it. Although live individuals may not be victimized in such cases, businesses and governments who are defrauded suffer losses. According to an Australian government publication, “One Melbourne offender obtained the birth certificates of four babies who had died in the 1970s and then, over eight months, claimed \$20,857 in unemployment benefits in their names. When arrested, the offender had with him a bag full of false proof of identity documents to support his welfare claims. These included motor vehicle learner’s permits, mobile phone accounts, student cards, rental documents and bank account access cards.”<sup>17</sup>

In a scam discovered by Canadian police, detailed identity documentation for individuals who had died as children was being sold for use by foreign individuals of roughly the same age, who then were able to obtain Canadian passports and other official documentation using their own photographs together with the name, date and place of birth and other information about the victim. Using this documentation, they were able to access Canadian medical care.<sup>18</sup>

<sup>12</sup> Javelin Strategy and Research, News Release: “Recent Javelin Study Shows Children Are At Risk for Identity Theft” (28 October 2008).

<sup>13</sup> FTC, Consumer Fraud and Identity Theft Complaint Data, January (December 2007), page 15.

<sup>14</sup> Criminal Intelligence Service Canada, *Annual Report 2008*, “Feature Focus: Identity Theft and Identity Fraud in Canada”.

<sup>15</sup> Home Office Statistical Bulletin, Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (15 May 2007), page 35.

<sup>16</sup> Experian UK, Press Release (8 October 2008).

<sup>17</sup> Australian National Crime Prevention Programme, *Identity Theft Information Kit* (May, 2004), available online at: <http://www.crimereduction.homeoffice.gov.uk/theft1.htm>.

<sup>18</sup> Joe Pendleton, Director of Special Investigations, Service Alberta, “The Growing Threat of Medical Identity theft in Canada”, Presentation to the Electronic Health Privacy Conference, Ottawa, (3 November 2008), available online at: <http://www.ehip.ca>; reported in Pauline Tam, “ID theft Scams Target Canada’s Healthcare System”, *The Ottawa Citizen* (3 November 2008).

### *Synthetic identities*

Identity criminals often create fictional identities by combining real and false information, or information from more than one victim. Indeed, it is now estimated that such “synthetic” identity fraud accounts for half of all identity fraud in the United States.<sup>19</sup> Synthetic identity fraud can be more difficult to detect than “true name” identity fraud, since records of the fraudulent activity do not immediately show up on victim credit reports or other records under the victim’s name.

In typical synthetic identity fraud now common in the United States, the thief combines one victim’s Social Security Number (“SSN”) with another person’s name and date of birth. Although the real SSN holder may not be affected by the subsequent frauds using her SSN, she may eventually be associated with them if creditors, debt collectors, tax authorities, law enforcement agencies or other authorities pursuing the fraud link the SSN back to her name. Such cases can be particularly damaging and difficult for victims to resolve given the delay in detection and the often confusing combination of identity information.<sup>20</sup>

Even if individuals whose identity information is used in synthetic identity fraud are not adversely affected by it, this form of identity fraud is extremely costly to businesses, consumers and the economy generally.

## 2. Victim typologies

Victims of identity-related crime can be categorized in a variety of different ways. Each typology provides insights into identity crime victims that can be useful in developing policy responses. The typologies discussed below categorize victims according to: (a) nature of the wrongful act; (b) method use to gather/steal the data: victim responsibility; (c) nature of damage suffered; (d) extent of damage suffered; (e) scale of crime; and (f) perpetrator identifiability/relationship with victim.

### *By nature of wrongful act*

Identity-related crime takes many different forms. The impact on victims varies depending on the nature of the crime, as do the appropriate approaches to prevention and remediation. It can therefore be useful for policy purposes to categorize victims according to the nature of the crime in question. However, neatly classifying victims in this way can be difficult given that many cases involve overlapping types of fraud.<sup>21</sup>

The United States Federal Trade Commission (“FTC”) separates identity-related crime (which it calls “identity theft”) into four categories: “existing credit card accounts”,

<sup>19</sup> Allen Jost, Vice-President, Business Strategy, ID Analytics; telephone interview (3 February 2009).

<sup>20</sup> See Leslie McFadden, “Detecting Synthetic Identity Fraud”, available online at: [http://www.bankrate.com/brm/news/pf/identity\\_theft\\_20070516\\_a1.asp](http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp) (16 May 2007).

<sup>21</sup> Synovate, *2006 Identity Theft Survey Report*, prepared for the Federal Trade Commission (November 2007) [“Synovate”], figure 2, page 13; Identity Theft Resource Center, *Identity Theft: The Aftermath 2007*, [“ITRC, Aftermath”] Tables 1A and 1B.

“existing non-credit card accounts”, “new accounts”, and “other”. This categorization reflects current incidence levels in the United States. Non-economic identity fraud includes State benefits fraud, employment fraud, tenancy fraud, real estate fraud, postal fraud, tax fraud and criminal evasion fraud. Such identity frauds are often committed by those seeking to avoid detection by authorities, such as illegal immigrants, drug couriers and criminals engaged in money-laundering.<sup>22</sup>

In some cases, there is no fraudulent use of the victim’s identity information. Instead, the unauthorized acquisition, transfer and/or use of that information is the only wrongful act in question.

The following is a typology of victims by nature of the wrongful act:

***Mere unauthorized acquisition, transfer and/or manipulation of identity information***

A necessary preliminary stage for identity fraud is the acquisition of another person’s identity information. This may be done in lawful or unlawful ways, with or without the victim’s knowledge, directly from the victim or from another source. Even if the act of acquiring is not unlawful (e.g., sifting through trash, taking advantage of security breaches), it is rarely authorized by the victim. If discovered, the mere taking of their identity information by a stranger—or even the mere exposure of their data to potential unauthorized access by criminals—can leave victims with a sense of violation and anxiety over potential fraudulent uses of the information.

Once acquired, identity information may be traded on the black market, used to create synthetic identities, or otherwise manipulated for future fraudulent use. Victims are unlikely to be aware of such activities unless and until they result in some form of fraud.

***Economic/financial fraud***

The most common form of identity-related crime reported in North America and the United Kingdom is that conducted for financial gain (usually referred to as “financial identity fraud”, but referred to here as “economic fraud”, consistent with the terminology adopted by the UN ODC).<sup>23</sup> This reflects the existence of mature credit markets and easy consumer access to credit in such economies, providing identity criminals with extensive opportunities to take advantage of a system designed to facilitate credit. Economic fraud can be divided into two distinct categories: *access to existing accounts* and *creation of new accounts*.

***Existing accounts***

CIFAS, the United Kingdom Fraud Prevention Service, reports significant increases in fraudulent use of existing accounts, distinguishing between “account takeover”, for which there was a 207 per cent increase in 2008 over 2007, and “account misuse”, for which there was a 69 per cent increase over the same period.<sup>24</sup>

<sup>22</sup> United Kingdom Cabinet Office, *Identity Fraud: A Study* (July 2002).

<sup>23</sup> ITRC, *Aftermath*, Tables 1A and 1B; European Fraud Prevention Expert Group, *Report on Identity Theft/Fraud* (22 October 2007) [“FPEG”], pages 8-9.

<sup>24</sup> CIFAS, Press Release: 2008 Fraud Trends (26 January 2009). In “account takeover”, perpetrators use information about the victim to divert and operate the account fraudulently for their own benefit. In contrast, “account misuse” simply involves the fraudulent use of an existing account such as a payment card or mail order account.

*Payment cards and devices:* The most common form of identity fraud reported in North America is unauthorized use of another person's credit card. "Plastic card fraud" is also a leading form of identity fraud reported in the United Kingdom. For the most part, the direct costs of such fraud are borne not by the individual victim but by credit card companies,<sup>25</sup> who then pass on these costs to their cardholders generally through high interest rates. Some stakeholders do not consider this form of identity fraud to be true identity fraud because it does not involve impersonation of the victim other than to access the account in question and generally has limited or easily repairable consequences for individual victims. However, payment card fraud causes significant damage to the defrauded businesses and to economic systems generally.

*Other existing accounts:* Fraudsters also use identity information of victims to access their bank or investment accounts (through debit cards, online banking, electronic funds transfer, cheque fraud or otherwise) and telephone accounts. Individual account-holders are less protected from liability for losses from this type of account fraud, although the financial industry is increasingly adopting codes of practice that protect consumers from liability for fraudulent electronic transactions unless it can be shown that the consumer acted without reasonable care.<sup>26</sup> In the United States, consumers are protected by law from liability for unauthorized electronic fund transfers depending upon the timing of consumer notice to the applicable financial institution.<sup>27</sup>

#### *New accounts*

Criminals frequently open up new financial accounts in the names of individual victims. Credit card, utility and telephone fraud are the most common forms of new account fraud in the United States. Criminals use personal information of victims to open up new accounts in their names and run up bills without paying.

Bank loans and mortgages are also taken out in the names of victims, who then suffer the consequences of the borrower defaulting.

#### ***Benefits fraud***

Identity criminals use the personal information of others in order to obtain government benefits, health services, and tax refunds, as well as drivers' licenses, passports and other government-issued documents. In the case of government-issued documents, criminals often impersonate deceased individuals in order to minimize chances of the fraud being discovered. For example, United Kingdom citizens have been contacted by the police to answer for crimes allegedly committed by a child of theirs who died in infancy.<sup>28</sup> Counterfeit documents are also frequently used to access services.

<sup>25</sup> For example, the United States Truth in Lending Act limits consumer liability for unauthorized credit card charges to a maximum of \$50: 15 USC. § 1601 et seq., implemented by Regulation Z, 12 C.F.R. § 226; see especially 15 USC. § 1643; 12 C.F.R. § 226.12(b). Similar laws exist in Canada. Credit card companies have adopted zero liability policies that further limit consumer liability for fraudulent transactions.

<sup>26</sup> See, for example, the United Kingdom Banking Code (March 2008), ss.12.11–12.13, available online at: [http://www.bba.org.uk/content/1/c6/01/30/85/Banking\\_Code\\_2008.pdf](http://www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf).

<sup>27</sup> *Electronic Fund Transfer Act*, 15 USC. § 1693 et seq., implemented by Regulation E, 12 C.F.R. § 205; see especially 15 USC. § 1693g; 12 C.F.R. § 205.6(b).

<sup>28</sup> United Kingdom Cabinet Office, *Identity Fraud: A Study* (July 2002), paragraph 1.2.



### ***Identity-related tax fraud***

This form of identity fraud has increased dramatically in the United States in recent years, as criminals obtain tax refunds using the identities of lawful taxpayers, claiming multiple dependents, phony working hours, and other details designed to maximize the refund.<sup>29</sup> Illegal immigrants or others may use stolen identities to obtain employment and then disappear without paying taxes owing, leaving the victim with a large outstanding tax bill. One United States taxpayer was reportedly faced with a \$1 million back-tax bill, even though she was a stay-at-home mother. An investigation later found that 218 illegal immigrants were using her Social Security Number. From 2002 through 2005, multiple identity criminals used the name and Social Security number of a Mexican-American factory worker to get jobs in Kansas, Texas and New Jersey. The victim had to deal with repeated allegations of under-reported income and long delays in receiving tax refunds owing to him.<sup>30</sup>

### ***Medical identity fraud***

Healthcare fraud is a particular concern in the United States, where universal health insurance is not provided by the State.<sup>31</sup> Criminals use the identities of others in order to obtain drugs, expensive medical treatment or fraudulent insurance payouts, leaving the victim with medical bills, corrupted medical records, and/or difficulties maintaining or obtaining health insurance.

For example, one American found that he was a victim of medical identity fraud when he received a call from a collection agency demanding payment of a bill for \$41,188 from a hospital he had never set foot in. Someone had used his name and Social Security Number to obtain surgery. Two years later, he was still suffering from a damaged credit rating, was “desperately trying not to go bankrupt”, and didn’t know if his medical records had been cleared.<sup>32</sup>

There is also evidence of a black market in Canadian citizenship documents (using the identities of deceased children), by which uninsured Americans fraudulently access the state-funded Canadian healthcare system.

### ***Drivers’ license fraud***

This form of identity fraud may leave victims with poor driving records and unpaid fines, leading to suspension or revocation of the victim’s license. According to a Canadian organization, “Often victims of identity theft & fraud first discover there is a problem when they go to renew their car insurance or driver’s license because outstanding fines must be paid before they will be allowed to renew insurance or a driver’s license”.<sup>33</sup> Identity criminals also use drivers’ license information to engage in other fraudulent activity, taking advantage of widespread use of drivers’ licenses for authentication purposes.

But even where it does not involve impersonation of live victims, drivers license fraud creates public safety risks and significant costs to the public treasury. In the United

<sup>29</sup> Federal Trade Commission, Consumer Fraud and Identity Theft Complaint Data, January–December 2007 [“FTC, 2007 Complaint Data”].

<sup>30</sup> Kevin McCoy, “Identity thieves tax the system”, *USA Today* (10 April 2008).

<sup>31</sup> See: <http://www.worldprivacyforum.org/medicalidentitytheft.html>.

<sup>32</sup> Max Alexander, “Your Medical Records, Stolen!”, *ReadersDigest.com*.

<sup>33</sup> British Columbia Crime Prevention Association, *Identity Theft Victim’s Toolkit* (February 2007).

Kingdom, it is estimated that detection and investigation of identity fraud in drivers' license application and testing processes cost the government £7 million per year.<sup>34</sup>

### ***Real estate fraud***

This type of identity fraud involves fraudsters using stolen identities or forged documents to transfer a registered owner's title to themselves without the registered owner's knowledge. The fraudster typically then obtains a mortgage on this property and once the funds are advanced on the mortgage, he or she disappears. Victims of this kind of fraud may lose their title to real estate.<sup>35</sup> A Canadian homeowner had to take her case to the province's highest court in order to regain title to her home after someone posing as her had transferred title to another imposter, who obtained a large mortgage on the property and then disappeared.<sup>36</sup> Real estate fraud is now a serious issue in Canada, and tops the United States Identity Theft Resource Center's list of predictions for 2009.<sup>37</sup>

### ***Employment fraud***

The United States has seen a marked increase in employment fraud in recent years, with criminals impersonating United States citizens (e.g., using the Social Security Numbers of children) in order to obtain work that they could not otherwise get legally, and/or to work without paying taxes.<sup>38</sup> This type of fraud can leave victims with a tax bill on earnings they did not receive, and without access to government benefits.

### ***Tenancy fraud***

Individuals with criminal or bad credit histories also impersonate others in order to obtain rental accommodation. Victims may be left with a record of unpaid rent, damaged property or other tenancy-related problems.

### ***Criminal evasion fraud***

Criminals may impersonate another person in order to evade law enforcement authorities. Victims of criminal identity fraud have been apprehended, detained and arrested for crimes that they never committed. For example, a United States mother of two was arrested and briefly jailed in 2008 for a burglary committed in her name. The real criminal had used identity information stolen from the victim's car four years previously. The victim had to spend \$3500 on legal fees in order to clear her name.<sup>39</sup>

### ***Postal fraud***

A common tactic of identity criminals is to redirect their victims' mail by filing a change of address notice in the name of the victim. This type of fraud is typically an intermediate stage in larger fraud schemes, allowing the thieves to collect more personal information about their victims for further fraudulent use.

<sup>34</sup> United Kingdom Identity Fraud Steering Committee, "New Estimate of Cost of Identity Fraud to UK Economy" (9 October 2008).

<sup>35</sup> Law Society of Upper Canada, Report to Convocation, *Mortgage Fraud* (24 March 2005).

<sup>36</sup> Dale Anne Freed, "Mortgage Fraud Victory; Woman wins back home as court reverses decision", *The Toronto Star* (7 February 2007).

<sup>37</sup> Ibid.; "Mortgage fraud hits \$1.5b. per year", *Calgary Herald* (18 March 2006); Identity Theft Resource Center, Press Release "Identity Theft Predictions 2009" (18 December 2008).

<sup>38</sup> FTC, 2007 Complaint Data.

<sup>39</sup> Reported on KVBC TV, Las Vegas NV (13 May 2008), accessed 31 January 2009 online at: [www.youridentitysafe.com](http://www.youridentitysafe.com).

### *By method used to gather/steal the data: victim responsibility*

Categorizing individual victims of identity theft by the method used can be helpful in assessing victim responsibility, as it allows for a rough differentiation among cases according to the level of control that the victim had to prevent the theft and/or fraud from occurring in the first place. This analysis should be approached with caution, however, as even when information is taken directly from the victim, it may be unfair to treat the victim as solely responsible. This is the case where, for example, the method used was surreptitious or difficult to detect, or where the method involves third party services (e.g., computer hardware and software, online banking) advertised and sold to the victim without adequate warning or instructions for preventing fraudulent use.

#### ***Victim negligence***

Identity thieves take advantage of carelessness on the part of individuals when they gather identity information through methods and from sources such as the following:

- Finding lost wallet, account/password information;
- Sifting through trash;
- Theft—stealing wallet, cheque-book, credit card, mail;<sup>40</sup>
- Eavesdropping on insecure wireless communications;<sup>41</sup>
- Personal websites;
- Social networking sites.<sup>42</sup>

#### ***Victim deception***

In many cases, victims are tricked into providing their data, either directly to the fraudster or via surreptitious computer programmes or corrupted electronic payment mechanisms. Depending on the context and the deceptive conduct in question, it can be unfair to attribute responsibility to the victim. Such methods of identity theft include:

- “Social engineering”: deceiving victims into providing sensitive data by posing as a trusted third party by phone, e-mail (“phishing”), or instant messaging (“SMSishing”);
- “Skimming” bank cards—via ATMs, hidden machines;
- Installing malware on victim computer surreptitiously (e.g., when victim downloads other applications) and using it to gather victim information through such means as keystroke logging or “click-jacking”.<sup>43</sup>

#### ***Third party public disclosures***

In some cases, individual identity data is made publicly available by third parties, often without the individual’s knowledge or consent. Organizations, both public and

<sup>40</sup> There may be little that a victim could have done to prevent theft.

<sup>41</sup> Wireless service providers bear some responsibility for properly informing individuals of the risks involved with insecure wireless communications, and providing simple means of securing the communications.

<sup>42</sup> Social networking sites bear some responsibility for warning users, especially young people, of the risks entailed with posting personal information on the site.

<sup>43</sup> Embedding concealed links that execute without the user’s knowledge when the user clicks on visible links on a webpage.

private, often fail to consider the ramifications of posting personal data online. Identity criminals can take advantage of information made public available via:

- Online public records (e.g., courts/tribunals);
- Employer/association websites;
- Post-disaster missing person sites;
- Obituaries.

### ***Third party negligence/deception***

Much of the data used by identity criminals (especially payment card and account data) is gathered from third parties, though a variety of means including those listed below. In such cases, individual victims have no ability to prevent the theft and often do not even know about it.

- Sifting through trash (“dumpster diving”), used computer equipment;
- Stealing computers, files;
- Bribing employees to collect and provide customer data;
- Duping employees (“pretexting”) in order to obtain customer data;
- Purchasing/subscribing fraudulently to databroker services;
- Hacking into computer systems/databases;
- Taking advantage of security breaches.

### *By nature of damage suffered to individuals and businesses<sup>44</sup>*

Because any one instance of identity-related crime may cause many different types of damage to a single victim, it can be difficult to categorize victims neatly by the type of damage suffered. Nevertheless, this typology is particularly useful for purposes of designing victim remediation programmes as it distinguishes among different types of damage suffered by victims, each of which requires different remediation measures.

#### ***Individuals***

##### *Direct financial loss*

Individual victims may incur direct financial loss in the form of debts fraudulently incurred, related fees, costs of mitigating damage (e.g., credit monitoring) and restoring records, or loss of title to real estate.

One United States survey estimates that identity-related crime cost individual victims an average of \$691 (with more than half incurring no expenses) in 2007,<sup>45</sup> while a 2006 survey commissioned by the FTC found that 10 per cent of identity crime

<sup>44</sup> For the purposes of this typology, we look at organizations (public and private) as well as individual victims.

<sup>45</sup> Javelin Strategy and Research, News Release: “Identity Fraud, Part 1: A \$45 Billion Snowball” (27 September 2008).

victims reported out-of-pocket expenses of \$1,200 or more, and the top 5 per cent incurred expenses of at least \$5,000.<sup>46</sup> A third United States survey found that the average loss to victims was \$3,257 in 2006, up from \$1,408 in 2005, while the percentage of funds consumers managed to recover dropped from 87 per cent in 2005 to 61 per cent in 2006.<sup>47</sup> Victims who contacted the United States Identity Theft Resource Center in 2007 spent an average of \$550 in out-of-pocket expenses for damage to an existing account, and \$1,865 to clear up new accounts fraudulently opened in their names.<sup>48</sup>

According to a recent Canadian survey, victims of identity-related crime spent a total of over \$155 million to resolve problems associated with the crime, with a mean cost per victim of \$92, or \$151 excluding credit card fraud.<sup>49</sup>

#### *Indirect financial loss*

The indirect financial costs of identity-related crime are often higher than the direct costs to individuals. Indirect costs include higher insurance rates and interest rates; being denied credit; being unable to use existing credit cards, being unable to obtain loans, difficulties obtaining or accessing bank accounts, and lost income (due for example to reputational damage or time taken off work).<sup>50</sup> A significant number of victims in the United States report difficulties getting credit agencies to remove inaccurate information from their files, or stopping them from putting negative information back in their records.<sup>51</sup>

#### *Reputational damage*

Individual victims of identity fraud suffer reputational damage of various sorts that can cause serious difficulties in obtaining or maintaining credit, employment, accommodation, health insurance, other insurance, drivers' licenses, passports, and other government identity or institutional (e.g., educational) documents. Reputational damage can also cause difficulties travelling across borders. Most devastating can be the damage caused to family or social relationships, especially when victims are arrested for crimes they never committed. For example, a United Kingdom citizen lost his job and was cut off by family members after being arrested for child pornography—an identity fraudster had used his credit card details to access a child porn website.<sup>52</sup>

#### *Inaccurate health records and/or inability to get health insurance*

Medical identity fraud can lead to serious consequences for health treatment if the victim's health records are inaccurate, or if the victim is unable to get needed health-care because of unpaid bills incurred in their name. This is unlikely to be a problem in states with publicly-funded healthcare, except to the extent that foreigners engage in identity fraud in order to access the publicly-funded healthcare system.<sup>53</sup>

<sup>46</sup> Synovate, page 6.

<sup>47</sup> Gartner, News Release (6 March 2007).

<sup>48</sup> ITRC, *Aftermath*, Executive Summary.

<sup>49</sup> Sproule and Archer, page 17.

<sup>50</sup> Synovate, page 7.

<sup>51</sup> ITRC, *Aftermath*, Executive Summary.

<sup>52</sup> Marc Sigsworth, "I was falsely branded a paedophile", BBC News online, 2008/04/03.

<sup>53</sup> As noted above, there is evidence of United States citizens fraudulently accessing the Canadian healthcare system using the identities of deceased Canadians.

*Wrongful detention/arrest*

Many United States citizens have been arrested for crimes committed by others who successfully impersonated them using stolen identity information. An alarming 62 per cent of respondents to a recent survey of victims by the United States Identity Theft Resource Center reported that criminals had committed financial crimes resulting in warrants being issued in the victim's name—more than 2.5 times higher than in 2006 and double the amount from 2004.<sup>54</sup>

*Harassment by collection agencies*

Victims of economic identity fraud often discover the problem only when they start receiving calls from collection agencies demanding payment of bills they never incurred or loans they never took out. According to the United States Identity Theft Resource Center's 2007 victim survey, 82 per cent of victims found out about the identity crime through "an adverse action" as opposed to proactive notification by businesses or monitoring of their credit reports.

Collection agencies and creditors often refuse to clear victim records despite substantiating evidence. Over half of victim respondents to the United States Identity Theft Resource Center's 2007 survey said that collection agencies continued to pester them about fraudulently incurred debts after they explained the situation.

*Time and trouble restoring reputation*

It can take hundreds of hours over a period of several years for a victim of identity-related crime to finally correct all corrupted records and restore their reputation. Average time per victim, according to a 2007 survey, was 40 hours.<sup>55</sup> A Canadian survey estimates that victims there spent a total of 21 million hours restoring their identity information, 13 hours on average per victim, and 17 hours when credit card fraud is excluded.<sup>56</sup> Victims who contacted the United States Identity Theft Resource Center in 2007 reported spending an average of 116 hours to repair damage done to existing accounts, and an average of 158 hours to clear up fraudulently opened new accounts. Severe cases involved thousands of hours, or "too many to count". It took up to a year to correct the misinformation in 70 per cent of cases, one to two years in 12 per cent of cases, and two or more years in 19 per cent of reported cases.<sup>57</sup>

*Emotional/psychological distress*

The emotional/psychological damage suffered by victims of identity-related crime can be profound, especially for victims of more serious or intractable frauds.<sup>58</sup> Indeed, the mental distress experienced by some victims of identity-related crime has been likened to that of victims of violent crime. According to an American psychologist specializing in the treatment of crime victims, "many victims/survivors of identity theft suffer many of the psychological, behavioral, and emotional symptoms as victims/survivors of violent crimes... some victims become exhausted, physically destructive or consider suicide".<sup>59</sup>

<sup>54</sup> *Aftermath*, *op cit*.

<sup>55</sup> Javelin Strategy and Research, News Release: "Though national statistics are trending downward, millions of Americans still at risk for identity theft" (8 October 2008).

<sup>56</sup> *Sproule and Archer*, page 17.

<sup>57</sup> ITRC, *Aftermath*, Executive Summary.

<sup>58</sup> *Ibid.*, pages 26-29: "Emotional Impact on Victims".

<sup>59</sup> *Dr Charles Nelson*, quoted in ITRC, *Aftermath*, page 27.

“Anger is a really big theme, and a sense of terrible injustice”, says a Canadian researcher studying the effects of identity crime on victims. “It really can shake people’s trust in the system, and it isn’t just the fact that the perpetrator has stolen their identity. Victims can also feel frustrated and powerless as they try to restore their credibility.”<sup>60</sup>

One victim states: “I am 25 years old, young and healthy, I should be enjoying my life; but instead I am stressed and paranoid about my financial status, which was once excellent.”<sup>61</sup> Another states: “My identity theft occurred because of a ministry project I was involved with helping others ‘get back on their feet’. Since I discovered this the outrage sense of betrayal and victimization has caused my seizure disorder to come back again increasing the emotional strains along with many other things.” “It was violating. It was almost like I was raped, and nobody was doing anything about it”, says another victim. “I think it would have been easier to walk into my house and have it cleaned out—then at least I’d know what to do. I just remember crying a lot and thinking ‘Why? Why did this happen to me?’”

Even victims of mere identity theft in the absence of fraud can suffer significant distress worrying about the potential frauds that could be attempted in their name. One such victim, having been notified of a security breach involving her husband’s investment account information and subsequently of a fraudulent attempt to open an account in his name, writes: “We felt sick to our stomachs and utterly violated. We spent weeks imagining horror scenarios revolving around my husband’s good name and credit rating being tarnished—if not destroyed—by some virtual body snatcher.”<sup>62</sup> Another victim states: “It was horrible. It’s so violating. My case was really minor, except now I live in fear of what could happen in the future since my information is still out there.”<sup>63</sup>

## ***Businesses***

### *Direct financial loss*

When businesses are defrauded through the use of fabricated identities or the identities of deceased persons, they suffer the associated losses. As well, when the identity information of live individuals is used to access or open accounts, businesses will often indemnify affected customers for related losses. Businesses contacting the United States Identity Theft Resource Center in 2007 reported average losses of almost \$50,000.<sup>64</sup>

It is worth noting that although businesses are victims in such cases, they may be able to pass such costs on to the general consumer base through, for example, high interest rates. This will be the case where identity-related crime is an industry-wide problem (such as in the payment card industry).

<sup>60</sup> Jessica Van Vliet, quoted in Karen Kleiss, “Woman had her bank accounts drained, found herself under investigation for fraud”, *The Edmonton Journal*, 20 December 2008.

<sup>61</sup> *Aftermath*, page 31.

<sup>62</sup> Licia Corbella, “I.D. theft hits home”, *Calgary Sun* (23 November 2007).

<sup>63</sup> TTRC, *Aftermath*, page 31.

<sup>64</sup> *Ibid.*, highlights.

*Reputational damage*

Corporate victims of identity theft may suffer reputational damage as a result either of mistaken identity (for example, when their trademark is used fraudulently) or of consumer loss of confidence in their ability to prevent identity fraud.

*Loss of goodwill*

Reputational damage can lead to a loss of goodwill, as consumers switch to other providers perceived as less risky.

*Cost of upgrading systems to combat identity-related crime*

Forms and techniques of identity-related crime are constantly evolving and in some cases intensifying, requiring businesses to constantly evaluate and improve their protective systems.

***Governments/taxpayers****Financial drain on health/welfare systems*

When identity-related crime involves fraudulent access to government services or fraudulently obtaining state-issued documents, governments suffer damages, the cost of which is passed on to taxpayers.

*Inaccurate citizen records*

There are a number of possible consequences of inaccurate records caused by identity fraudsters, including:

- Damage to integrity of state records systems: health, social assistance/public benefits, drivers' license, passport/travel, tax, immigration, procurement;
- Compromised state security (e.g., terrorist watch lists);
- Compromised public safety (unsafe drivers, undetected criminals);
- Compromised immigration policy;
- Compromised health care;
- Loss of citizen confidence in state;
- Greater susceptibility to corruption and organized crime.

*Cost of upgrading systems to combat identity-related crime*

Like businesses, governments need to be constantly vigilant with respect to this evolving crime and must have effective systems in place to prevent, detect and mitigate it.

*Cost of law enforcement pursuing ID criminals*

Because of its often elaborate and sophisticated nature, identity-related crime requires a significant investment of law enforcement resources. Police forces have insufficient resources, both quantitatively and qualitatively, to investigate and prosecute this type of crime, especially when it involves organized groups of criminals operating across jurisdictions. This is the case globally as well as domestically, as increasingly sophisticated international mechanisms are needed for international cooperation in the investigation of identity-related crimes.



### *By extent of damage suffered*

Another possibly useful typology of identity crime victims is based on the extent of damage suffered. This approach takes into account the nature of the crime and the type of damage incurred, discussed above, but differs insofar as it focuses on the *extent* to which the victim suffers. By doing so, it can be helpful in deciding on how to prioritize individual victim remediation services, for example.

Two important caveats regarding this proposed typology are in order: First, this categorization ignores costs to businesses, governments, or the economy/consumers generally. Even where victims incur minimal damages, there is a substantial cost to affected businesses who may pass such costs on to consumers, or to governments who pass the costs on to taxpayers. Second, the subjective character of emotional/psychological distress—perhaps the most common and often most severe impact of identity-related crime on victims—can make it especially difficult to measure and thus determine in which category a given victim belongs.

Nevertheless, the following is a possible approach:

#### ***Minimal damage***

Victims of identity-related crime in this category suffer damage that:

- Results from a single act or set of acts involving a single account, transaction or relationship;
- Is easily and quickly rectified;
- Is fully compensated (monetary losses); and
- Involves no lasting damage to reputation or health.

Mere payment card fraud would fall into this category, as long as the victim is fully compensated.

#### ***Significant damage***

Victims in this category suffer damage that:

- Involves repeated acts involving more than one account, transaction or relationship; and
- Is difficult and time-consuming to rectify, or
- Involves no easily obtained compensation, or
- Is lasting (e.g., to reputation, health, etc.).

Most victims of identity-related crime likely fall into this broad category, which can be further broken down into the following sub-categories:

#### ***Significant damage—easily corrected***

Victims succeed in restoring their records without undue effort and suffer no lasting reputational or health damage.

*Significant damage—difficult to correct but no trauma*

Victims experience prolonged reputational/credit damage, must spend a significant amount of time restoring their records, or suffer significant financial losses, but do not experience severe emotional or psychological trauma.

*Significant damage—lasting trauma*

Victims experience severe trauma and/or significant and lasting damage to their health or reputations.

### *By scale of crime*

Identity-related crime can be either large-scale or small-scale. It can be as small in scale as a single criminal actor targeting a single victim, or as large as an international crime ring targeting millions of Internet users. Because large-scale frauds are more likely to be reported and acted upon by authorities, victims of such frauds may be more likely than victims of small-scale frauds to receive assistance.

But while the number of victims may be relevant with respect to economy-wide costs and thus to the allocation of scarce law enforcement resources, it is less relevant from the individual victim perspective. Even small scale identity fraud can be devastating to the victim if it involves the creation of extensive financial liabilities or full impersonation for the purposes of evading authorities.

### *By perpetrator identifiability/relationship with victim*

Studies from the United States and Canada suggest that a significant proportion of identity-related crime is perpetrated by individuals known to the victim, such as family members, acquaintances, neighbours, co-workers, and in-home employees.<sup>65</sup> However, recent statistics suggest that this figure is dropping and that the vast majority of victims know little or nothing about the identity of the perpetrator.<sup>66</sup>

Identifiability of the perpetrator is an important factor for victim remediation insofar as it facilitates criminal investigations and allows victims to pursue civil recourse. The more difficult it is to identify perpetrators, the more difficult it is to pursue and punish them. On the other hand, identity frauds conducted by perpetrators who are known to the victim may tend to take longer to detect, and can thus be more devastating for victims.<sup>67</sup>

<sup>65</sup> ITRC, *Aftermath*, table 7, pages 14-15; *Sproule and Archer*, pages 22-23.

<sup>66</sup> Synovate, page 28, figure 9; *Sproule and Archer*, pages 22-23.

<sup>67</sup> *Sproule and Archer*, page 23.

# III. LEGAL BASES FOR RESTORATION OF VICTIM IDENTITY

Victims of identity-related crimes experience notorious difficulty restoring their reputations and identity information. Convincing authorities that they are innocent, identifying and correcting corrupted records, dealing with sometimes byzantine bureaucracies, and preventing further fraud in their names are exhausting, time-consuming, and often extremely stressful. For some victims, the process of restoration never ends. The need to facilitate victim restoration and remediation cannot therefore be overstated.

There are a number of legal and quasi-legal bases upon which victims of identity-related crime can rely for various types of remediation. These include “victims’ rights” codes, laws and declarations; the availability of restitution under criminal law; civil law causes of action; and human rights to identity, privacy and reputation. Each of these is discussed below.

## 1. Normative basis for victim remediation: victims’ rights initiatives

### *United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*

In 1985, the General Assembly of the United Nations adopted the Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power.<sup>68</sup> This Declaration calls upon Member States to implement its provisions, which focus on victim assistance, treatment and remediation. Notable provisions of the Declaration in relation to identity crime victims include the following:

5. Judicial and administrative mechanisms should be established and strengthened where necessary to enable victims to obtain redress through formal or informal procedures that are expeditious, fair, inexpensive and accessible. Victims should be informed of their rights in seeking redress through such mechanisms.

[...]

<sup>68</sup> G.A. Resolution 40/34, (29 November 1985). Work is currently underway on a draft United Nations Convention on Justice and Support for Victims of Crime and Abuse of Power, with a view to stimulating further implementation of and compliance with the basic principles contained in the Declaration.

8. Offenders or third parties responsible for their behaviour should, where appropriate, make fair restitution to victims, their families or dependants. Such restitution should include the return of property or payment for the harm or loss suffered, reimbursement of expenses incurred as a result of the victimization, the provision of services and the restoration of rights.

[...]

12. When compensation is not fully available from the offender or other sources, States should endeavour to provide financial compensation to:

- (a) Victims who have sustained significant bodily injury or impairment of physical or mental health as a result of serious crimes;

[...]

14. Victims should receive the necessary material, medical, psychological and social assistance through governmental, voluntary, community-based and indigenous means.

[...]

16. Police, justice, health, social service and other personnel concerned should receive training to sensitize them to the needs of victims, and guidelines to ensure proper and prompt aid.

The Declaration defines “victims” broadly to include situations in which the perpetrator cannot be identified, apprehended, prosecuted or convicted, and regardless of the familial relationship between the perpetrator and the victim. However, like other statements and enactments of victims’ rights, it applies only to those who have suffered harm “through acts or omissions that are in violation of criminal laws operative within Member States”. Thus, to the extent that identity-related crimes are not recognized as offences in national laws, the United Nations Declaration is of little assistance.

Nevertheless, the United Nations Declaration provides a strong normative basis for victims of identity-related crime to demand state assistance and facilitation of the remediation process, especially where the crimes are recognized as such domestically.

#### *Other international resolutions, guidelines, etc.*

The United Nations ECOSOC Resolution 2004/26 on International Cooperation in the Prevention, Investigation, Prosecution and Punishment of Fraud, the Criminal Misuse and Falsification of Identity and Related Crimes explicitly encourages Member States “to facilitate the identification, tracing, freezing, seizure and confiscation of the proceeds of fraud and the criminal misuse and falsification of identity”, among other measures more preventative in nature. Criminal restitution can be helpful to victims in cases where perpetrators are prosecuted.

The Organization of Economic Cooperation and Development (“OECD”) has issued a number of relevant guidelines and recommendations to its Member States, including:

- The 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (discussed further, below, under “Data Protection”).
- The 2002 Guidelines for the Security of Information Systems and Networks, Principle 2 of which emphasizes the responsibility of those designing, supplying and operating information systems and networks, noting that “all participants are responsible for the security of information systems and networks” and that “participants should be accountable in a manner appropriate to their individual roles.” In other words, individual victims should only have to bear the burden of loss to the extent that they are responsible, and organizations whose negligence contributed to the theft or fraud should bear their fair share of such losses.
- The 2003 Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, which state among other things, that Member countries should:

“[establish] effective mechanisms that provide redress for consumer victims of fraudulent and deceptive commercial practices” (Part II.A.4.); and should “jointly study the role of consumer redress in addressing the problem of fraudulent and deceptive commercial practices, devoting special attention to the development of effective cross-border redress systems” (Part VI).
- The 2007 OECD Council Recommendation on Consumer Dispute Resolution and Redress, which sets out a number of specific recommendations designed to improve domestic and cross-border redress mechanisms, in addition to the general recommendation that:

“Member countries should review their existing dispute resolution and redress frameworks to ensure that they provide consumers with access to fair, easy to use, timely, and effective dispute resolution and redress without unnecessary cost or burden.

In so doing, member countries should ensure that their domestic frameworks provide for a combination of different mechanisms for dispute resolution and redress in order to respond to the varying nature and characteristics of consumer complaints.”

### *Domestic initiatives to assist victims of identity-related crime*

Consistent with the United Nations Declaration, many States have taken measures to assist victims of crime, including the enactment of victims’ rights laws.<sup>69</sup> Despite their titles, such laws do not usually create enforceable rights for victims; instead, they typically provide for victim support services, allow for victim impact statements at court hearings, and establish regimes under which certain kinds of victims can apply for financial assistance or compensation (see below).<sup>70</sup>

<sup>69</sup> For example, New Zealand, Victims’ Rights Act, 2002.

<sup>70</sup> See, for example, James Blindell, Review of the Legal Status and Rights of Victims of Identity Theft in Australasia, Australasian Centre for Policing Research, Report Series No. 145.2 (2006).

Non-legislated principles, similar to those in the United Nations Declaration, have also been formally adopted by some jurisdictions, providing for example, that victims should have access to various kinds of support and protection services; should be kept informed, upon request, about the progress of the investigation and prosecution; and should have their views and concerns taken into consideration by investigators and prosecutors.<sup>71</sup>

While such victims' rights initiatives may be helpful to victims in some cases of identity-related crime, they are in general targeted at different types of crime and do not address the primary needs of identity crime victims, which include, first and foremost, restoration of reputation and of the integrity of corrupted identity information.

Either as part of a victims' rights law or separately, many states have instituted criminal injuries compensation regimes, under which victims of violent crimes may be compensated for their suffering. Individuals must apply to the relevant authority for compensation, which may or may not be granted. Such compensation is however generally available only to victims and families of victims who suffer serious physical injury, emotional trauma or death as a result of violent crime.<sup>72</sup> Given the narrow focus of these regimes on violent crime, it is unlikely that victims of identity-related crime would qualify for such compensation.

## 2. Legal basis for restoration: criminal law

### *International criminal law conventions*

Efforts are underway to implement the United Nations Declaration on the Basic Principles of Justice for Victims of Crime and Abuse of Power through a new United Nations Convention.<sup>73</sup> In the meantime, some existing international Conventions applicable to identity-related crime address victim issues to varying degrees. Perhaps most relevant is the United Nations Convention Against Transnational Organized Crime<sup>74</sup> ("Palermo Convention"), which explicitly provides for "Assistance to and protection of victims" in Article 25 as follows:

1. Each State Party shall take appropriate measures within its means to provide assistance and protection to victims of offences covered by this Convention, in particular in cases of threat of retaliation or intimidation.
2. Each State Party shall establish appropriate procedures to provide access to compensation and restitution for victims of offences covered by this Convention.
3. Each State Party shall, subject to its domestic law, enable views and concerns of victims to be presented and considered at appropriate stages of criminal proceedings against offenders in a manner not prejudicial to the rights of the defence.

<sup>71</sup> Ibid.

<sup>72</sup> *Blindell, op cit.* See also legislative regimes for criminal injuries compensation in Canada and the United States.

<sup>73</sup> International Victimology Institute, Tilburg University ("INTERVICT"), available online at: <http://www.tilburguniversity.nl/intervict/undeclaration/>. The current draft Convention is entitled "United Nations Convention on Justice and Support for Victims of Crime and Abuse of Power".

<sup>74</sup> G.A. Resolution 55/25 (15 November 2000).

Both the Palermo Convention and the United Nations Convention Against Corruption<sup>75</sup> (“Merida Convention”) include provisions for returning confiscated property or proceeds of crime to requesting State Parties so that they can compensate victims of crime or return such property or proceeds to their legitimate owners.<sup>76</sup> The Palermo Convention also requires that State Parties develop or improve specific training programmes dealing among other things with “methods used in the protection of victims and witnesses”.<sup>77</sup>

### *Restitution under domestic criminal law*

As discussed below under “Best Practices”, some jurisdictions provide for victim restitution under their criminal laws. Restitution is typically available only in cases of criminal conviction, and only for certain types of crimes. Moreover, it is often limited to compensation for actual expenses incurred as a direct result of the crime.

Criminal restitution is therefore available to victims of identity-related crime only in the rare cases in which the perpetrators are prosecuted under criminal law and that result in a conviction. It requires that the criminal be able to pay, which is not always the case. Furthermore, if limited to compensation for documented, out-of-pocket expenses, it is of little value where the victim’s main damages are emotional and/or related to time spent and lost income. Finally, criminal restitution is of limited value insofar as it does not restore the victim’s identity information and reputation.

## 3. Legal basis for restoration: civil law

### *Credit reporting legislation*

Credit reporting laws regulate the activities of credit reporting agencies, i.e., agencies that create, administer, and provide access to the financial credit histories of individual consumers. Such agencies are a mainstay of modern credit-based economies and key players in economic identity fraud insofar as they collect, hold and disclose the fraudulent data that results in victimization. The laws governing these agencies typically place limits on the information that can be gathered and to whom it may be disclosed, require that the agency take all reasonable steps to ensure that the information it holds is accurate and fair, and give consumers a right to access their reports and have errors corrected.<sup>78</sup>

In response to the recent increase in identity-related economic fraud, credit reporting laws in a number of North American jurisdictions have been amended to, among other things, provide victims of identity theft with the ability to put a “fraud alert” and/or a “freeze” on their credit files, thus limiting the ability of criminals to obtain credit in their name. Such laws are critical tools for victims of economic identity fraud in detecting and preventing

<sup>75</sup> G.A. Resolution 58/4 (31 October 2003).

<sup>76</sup> Palermo Convention, Article 14(2); Merida Convention, Article 57(3)(c).

<sup>77</sup> Article 29(1)(i).

<sup>78</sup> For example, Fair Credit Reporting Act, 15 USC. § 1681 et seq.; Ontario Consumer Reporting Act, R.S.O. 1990, c.C-33.

further fraud, and are discussed in more detail in the next section, under “Best Practices—Credit Reporting Agencies”.

Credit reporting legislation thus provides victims with direct rights to control the sharing of their financial data and to restore their financial records. Other civil laws, discussed below, provide victims with indirect rights to redress through formal complaints to authorities or through civil actions.

### *Consumer protection legislation*

Consumer protection legislation is also relevant insofar as it provides consumers who become victims of identity-related crime recourse with respect to debts fraudulently incurred.<sup>79</sup> In some States, consumers are protected by law from liability for the cost of fraudulent transactions by identity criminals in certain situations. For example, in the United States, consumer liability for unauthorized credit card charges is limited to \$50 as long as the credit card company is notified within 60 days, and liability for unauthorized debit card charges is limited to \$50 if reported within two business days, and to \$500 if reported later. Under the European Council Directive concerning the distance marketing of consumer financial services, “Member States shall ensure that appropriate measures exist to allow a consumer to request cancellation of a payment where fraudulent use has been made of his payment card in connection with distance contracts covered by this Directive, and in the event of fraudulent use, to be re-credited with the sums paid or have them returned.”<sup>80</sup>

### *Data protection laws*

Flowing from the broader right to privacy discussed below is a large and growing body of domestic, regional, and international data protection laws and guidelines, applicable to both the private and public sectors.<sup>81</sup> These laws are particularly relevant to victims of identity-related crime as they are designed precisely to protect against such crime and other abuses of one’s personal data. In addition to establishing obligations of data protection applicable to public and private sector entities, they usually provide individual victims with an avenue through which to seek redress.

### *Legal basis of data protection laws*

International documents requiring the adoption of data protection laws domestically or designed to assist states in the drafting of data protection legislation include the following:

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980);<sup>82</sup>

<sup>79</sup> Such legislation also appears in the inventory of public sector practices for victim remediation, below.

<sup>80</sup> Directive 2002/65/EC, Article 8.

<sup>81</sup> Electronic Privacy Information Centre and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007). [“EPIC et al”].

<sup>82</sup> See: [www.oecd.org](http://www.oecd.org).



- Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981);<sup>83</sup>
- United Nations Guidelines Concerning Computerized Personal Data Files (1990);<sup>84</sup>
- European Community Directive on the Protection of Personal Data with regard to the processing of personal Data the Free Movement of Such Data (“Data Protection Directive”) (1995);<sup>85</sup>
- Asia Pacific Economic Cooperation (APEC) Privacy Framework (2004).<sup>86</sup>

The number of countries that have adopted comprehensive or sectoral data protection laws governing the private sector has increased exponentially over the past decade, due in large part to the dramatic increase in risks such as identity-related crime that have been created by the computerization of data and huge growth in transborder data flows.

### Content of data protection laws

Such laws are built upon the principles set out in the OECD Guidelines and Council of Europe Convention, among other documents.<sup>87</sup> These principles govern the collection, retention, use and disclosure of “personal data”, which is generally defined as information of any sort and in any form about an identifiable individual. Fair information principles, as set out in the OECD Guidelines and related documents include:

- *Collection limitation* (only collecting personal data by fair and lawful means, with consent of data subject where appropriate, and/or only as necessary for identified purposes);
- *Data quality* (personal data should be accurate, complete and up-to-date to the extent necessary for purposes);
- *Purpose specification* (purposes for which personal data is collected should be specified before or at the time of collection; new purposes require new specification);
- *Use limitation* (no use or disclosure of personal data without consent of the data subject or by authority of law);
- *Security safeguards* (personal data must be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure);
- *Openness* (data controllers should be open about their practices and policies with respect to personal data);
- *Individual participation* (individuals should have rights to access data about them held by the data controller and to have inaccurate data corrected);

<sup>83</sup> Council of Europe Convention No. 108 (18 September 1980).

<sup>84</sup> Adopted by General Assembly Resolution 45/95 (14 December 1990).

<sup>85</sup> Directive 95/46/EC.

<sup>86</sup> APEC Privacy Framework (2005).

<sup>87</sup> See, for example, the National Standard of Canada CAN/CSA-Q830-96, Model Code for the Protection of Personal Information, which has been adopted into law as Schedule 1 to the Personal Information Protection and Electronic Documents Act, S.C.2000, c.5.

- *Accountability* (data controllers should be accountable for complying with measures that give effect to these principles).

Many countries have adopted these or related rights and obligations into their domestic laws, either in the form of comprehensive, cross-sectoral data protection legislation (as in Europe, Canada, and Australia for example) or in sector-specific and issue-specific laws such as those governing the financial industry, health information, and children's online privacy in the United States.

### Applicability to identity-related crime

Informational privacy rights, in particular data protection laws, are directly relevant to victims of identity-related crime. These laws establish obligations of data minimization and data security precisely to protect such data from unauthorized access and use. The failure of organizations to fulfill their obligations under such laws is frequently a causal factor in identity-related crime.

Data protection laws require organizations to, among other things:

#### *Minimize data collection and retention*

Identity criminals thrive on the proliferation of increasingly large and rich databases of personal information created and maintained by public and private sector organizations. Although many such databases are carefully secured, there is no such thing as perfect security, and hardly a day goes by that one does not hear of a security breach exposing personal data to potential abuse by identity criminals. By simply not collecting personal data that they don't need, and by destroying it as soon as it is no longer needed, organizations would significantly reduce the risk of unauthorized access to or use of personal data in their possession. A recent large-scale case of identity theft and fraud in North America involved access by criminals to a large retailer's database of detailed customer credit card and other data, some of which should never have been collected in the first place and much of which should not have been retained for as long as it was.<sup>88</sup>

#### *Take reasonable steps to ensure data security*

This includes protecting the data from outside threats via, for example, computer firewalls, physical locks, and other methods; proper disposal of records and electronic media; and ensuring that staff is adequately trained and systems are monitored so as to prevent security breaches.

It also includes protecting the data from inside threats through such measures as employee screening and monitoring, and use of access controls so as to limit the ability of staff members to access personal databases.

Security measures also include effective authentication of those making requests for data or applying for services such as credit. Failure to properly authenticate applicants

---

<sup>88</sup> Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner of Alberta, Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies Inc./Winners Merchant International L.P. (25 September 2007).

for credit, government benefits, identity documents, or other services is a common feature of identity-related crime: the criminals succeed in the fraud because organizations allow them to.

#### *Notify individuals and authorities of security breaches*

With the recent rise in identity-related crime, security breach notification requirements have been adopted into legislation by many jurisdictions, and are being considered by many more. Security breach notification rules require that organizations notify affected individuals and relevant authorities of security breaches that expose personal data to unauthorized access and potential identity theft. Such rules achieve two purposes: allowing potential victims of identity theft to mitigate harm by taking strategic preventative action, and creating a stronger incentive for organizations to prevent such breaches in the first place (thereby avoiding the reputational damage and costs of notification).

### Rights to redress under data protection laws

Data protection laws involve a variety of enforcement regimes, some reliant on state enforcement and others reliant on private enforcement via a data protection authority and/or the courts. The effectiveness of these enforcement mechanisms varies by State, and both public and private enforcement models have been criticized for tolerating significant non-compliance.<sup>89</sup>

Under most data protection laws, individuals who suffer harm as a result of an organization's failure to comply with data protection law have a right to redress. Under some regimes, victims can lodge complaints and obtain binding orders from a special data protection authority established for this purpose.<sup>90</sup> Under other models, they must apply to the court for compensation or other enforceable remedies.<sup>91</sup> In most cases, their rights to redress are limited to compensation for damage suffered, which in some but not all regimes includes emotional damage.

There is little evidence of victims of identity-related crime taking advantage of these rights of recourse. This is likely because of a number of factors, including the low probability of obtaining a damage award that justifies the cost of litigation, as well as the victim's inability to determine how, when and where their information was obtained by the thief, and the consequent difficulty establishing a causal link between the fraud in question and an organization's non-compliance with data protection laws.

### *Other privacy laws*

In addition to data protection laws and constitutional rights, many jurisdictions have enacted in legislation or judicially recognized other privacy rights applicable to the private

<sup>89</sup> See, for example, *Chris Connolly*, *The US Safe Harbor: Fact or Fiction?* (Galexia, 2008), and CIPPIC, "Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up", (April 2006).

<sup>90</sup> For example, private sector data protection statutes in the provinces of Quebec, Alberta and British Columbia, Canada.

<sup>91</sup> This is the case under Canada's federal private sector law, the Personal Information Protection and Electronic Documents Act.

sector.<sup>92</sup> Many civil codes, for example, provide for an actionable right to privacy.<sup>93</sup> Such laws commonly prohibit and/or make actionable such privacy invasions as:

- Unauthorized use of a person's name or image for commercial or other gain;
- Eavesdropping, spying, or other forms of private surveillance;
- Surreptitiously listening to or recording private telecommunications; and
- Unauthorized use of person's personal letters, diaries or personal documents.

For example, a plaintiff in Quebec, Canada, succeeded in obtaining damages from a magazine that published a photograph of her on its cover without her authorization. The unauthorized publication of her photo was found to constitute a breach of her privacy under Quebec law and resulted in a damage award.<sup>94</sup>

Such actions are also possible under the tort of "misappropriation of personality" recognized by some common law courts.<sup>95</sup> The tort implicitly recognizes a right of individuals to control and market their own image. Individuals (often celebrities) whose images have been exploited in this manner have succeeded in obtaining damages to compensate them for loss of control over their image and loss of control over with whom or what that image is associated. Such misappropriation is clearly analogous to the misappropriation of identities in the context of identity-related crime, and it is possible that this tort could be developed so as to apply to identify thieves and fraudsters. Factors that could limit its use include the type and extent of the personal information misappropriated and of the harm caused to the victim.

There is also an emerging tort of invasion of privacy in some common law jurisdictions, which could potentially prove useful to victims of identity-related crime.<sup>96</sup> This cause of action treats intrusion into one's seclusion, solitude or private affairs as a civil wrong for which damages may be awarded.

More solid in law, however, are clear statutory privacy rights such as those in Quebec referred to above. There has been at least one identity fraud case successfully litigated under the French civil right to privacy, under which the perpetrator was ordered to compensate the victim for emotional duress and the public health insurance programme for related costs.<sup>97</sup>

While these laws provide victims of identity-related crime with a clear legal basis on which to obtain compensation for their losses (e.g., for unauthorized use of the victim's name and personal documents), they are useless unless the victim can identify the

<sup>92</sup> Four Canadian provinces (British Columbia, Manitoba, Newfoundland and Saskatchewan) legislated torts of privacy invasion actionable, without proof of damage, against any person who knowingly and without claim of right violates the privacy of another person. The province of Quebec prohibits similar acts of privacy invasion under its Civil Code (Articles 35, 36), as do many other civil law jurisdictions.

<sup>93</sup> For example, the French Civil Code, Articles 9 and 1382; Civil Code of Quebec, S.Q., 1991, c. 64, Articles 35, 36.

<sup>94</sup> *Aubry v. Editions Vice-Versa Inc.*, [1998]1 S.C.R. 591.

<sup>95</sup> See, for example, *Horton v. Tim Donut Ltd* (1997), 75 C.P.R. (3d) 467 (Ont.C.A.).

<sup>96</sup> Invasion of privacy has not traditionally been recognized as an independent tort in common law, but some courts (e.g., in Canada) are beginning to recognize it as such, noting the need for the common law to evolve consistent with constitutional values. See, for example: *Savik Enterprises Ltd v. Nunavut*, [2004] Nu.J. No. 1 (Nun.C.J.); *Somwar v. McDonald's Restaurants of Canada Ltd*, [2006] O.J. No. 64 (Ont. S.C.J.).

<sup>97</sup> See FIDIS, page 40.

perpetrator. Yet victims of identity fraud often cannot identify the wrongdoer. Even where they can, the wrongdoer may be “judgment proof” (i.e., unable to pay a court-ordered award) by the time the victim obtains a court order. Other factors such as low damage awards and the high cost of litigation also inhibit litigation by victims under these privacy laws.

### *Other civil laws*

#### **Causes of action against perpetrators**

##### *General tort law*

Tort law and other general civil laws include numerous causes of action, many of which are potentially applicable to perpetrators of identity-related crime. Such actionable wrongs under common law include misrepresentation, fraud, nuisance (interference with enjoyment of property), intentional or negligent interference with property (trespass), intentional infliction of emotional distress, and defamation.

An identity fraud victim can sue the perpetrator of the crime under such causes of action, seeking compensation for both economic damages and noneconomic damages, such as pain and suffering. Such causes of action are not very helpful, though, where the perpetrator is unknown, located in a far-flung jurisdiction, or otherwise difficult to identify or collect from.

##### *Defamation*

The law of defamation is designed to protect individuals and corporations from harm to their reputations by false and derogatory remarks about them. Defamatory remarks may be verbal (slander) or written (libel). They must be published or otherwise conveyed to a third party, and must be a direct attack on the victim in order to be actionable in law. Defamation is largely a civil law matter, but serious cases may, depending on the jurisdiction, also be treated as criminal offences.

Defamation is clearly analogous to identity fraud insofar as both cause injury to the reputation of victims. However, defamation requires written or spoken statements about the victim. In contrast, identity fraud typically harms reputation in an indirect manner, as a result of the actions rather than the statements of the wrongdoer. It may be possible, however, that the fraudulent signing of documents in another person’s name, or false credit reporting by a credit bureau, is found to constitute libel insofar as it causes harm to the victim’s reputation.<sup>98</sup> Defamation law may also be of use to victims of corporate identity theft, insofar as the fraudulent publication and use of a corporate name and logo results above all in reputational damage to the corporation.

##### *Intellectual property rights*

Victims of corporate identity theft/fraud (i.e., misappropriation of corporate identity) have rights under trademark laws to sue and recover damages from infringers of those

<sup>98</sup>We have found no case law or authoritative commentary on this.

rights. Trademark law is designed precisely to provide remedies for such infringement, and would appear to provide victims of corporate identity theft/fraud with a clear basis on which to sue infringers.<sup>99</sup>

Creators (individual and corporate) of works benefit from copyright laws designed to protect their works from unauthorized use. Depending on the jurisdiction, such rights include an author's economic right not to have their work presented in a manner harmful to their future sales, a celebrity's right not to have their physical image misused to create a false appearance of endorsement, and a moral right not to have works subjected to derogatory treatment.<sup>100</sup> Some instances of identity-related crime could involve infringement of these rights, but such instances are not widely reported in the literature on identity-related crime and are likely to be uncommon given that identity fraud does not usually involve the use of victims' creative works.

### Causes of action against organizations that facilitated the crime

Civil laws potentially applicable to organizations whose actions or omissions facilitated the identity-related crime are more likely to be useful to victims of identity-related crime since such organizations are relatively easy to identify, sue and collect from. Such causes of action include breach of contract, negligence and breach of confidence.<sup>101</sup>

In the United States, there have been a number of legal actions against third parties whose acts or negligence contributed to identity theft and fraud, some of which have been successful. Claims in these cases fall into four general categories: negligent security of personal information, negligent sale of information, failure of a bank to prevent identity theft/fraud or to mitigate damages, and liability of credit reporting agencies for failure to prevent or remedy incidents of fraud. As in claims for damages due to negligent security resulting in a violent criminal assault, the defendant is alleged to have failed to take reasonable precautions to protect the victim from foreseeable injuries caused by a third party.<sup>102</sup>

Under German civil law, courts have ruled that once an organization becomes aware that a prior account was fraudulently created in another person's name, it must take precautionary measures preventing a similar action concerning the victim.

Recovery of loss in either case requires that the victim prove that such negligence or breach contributed to his or her losses. Establishing a causal link is often difficult in the context of identity fraud, when the victim typically has little information about how the

<sup>99</sup> Microsoft, for example, has claimed trademark infringement in a number of lawsuits against people fraudulently posing as Microsoft in e-mail phishing scams. See, for example, *Todd Bishop*, "Microsoft casts net for phish culprits", *Seattle Post-Intelligencer* (1 April 2005).

<sup>100</sup> For example, s.14.1 of the Canadian Copyright Act, R.S.C. 1985, c.C-42. Although waivable under Canadian copyright law, moral rights are non-waivable in many other jurisdictions.

<sup>101</sup> The tort of "breach of confidence" protects private information that is conveyed in confidence, and a claim for breach of confidence typically requires that the information be of a confidential nature, that it was communicated in confidence, and that it was disclosed to the detriment of the claimant.

<sup>102</sup> See *Jeffrey Dion and James Ferguson*, "Civil Liability for Identity theft", (1 February 2007), available online at: [http://goliath.ecnext.com/coms2/gi\\_0199-6285492/Civil-liability-for-identity-theft.html](http://goliath.ecnext.com/coms2/gi_0199-6285492/Civil-liability-for-identity-theft.html). See also *Wood and Schecter*, "Identity Theft: Developments in Third Party Liability", American Bar Association, *Section of Litigation Consumer and Personal Rights Newsletter*, vol. VIII, No. 3 (Summer 2002), available online at: [http://www.jenner.com/files/tbl\\_s20Publications/RelatedDocuments PDFs1252/380/Identity\\_Theft.pdf](http://www.jenner.com/files/tbl_s20Publications/RelatedDocuments PDFs1252/380/Identity_Theft.pdf).

fraud was committed. Moreover, some courts are reluctant to award damages in tort law (negligence) for “pure economic loss” (i.e., financial loss other than that directly connected to physical damage to the victim or the victim’s property).<sup>103</sup> This doctrine further limits the ability of identity crime victims to redress under tort law.

### Inadequacies of litigation as an avenue of redress for victims of identity-related crime

As noted above, victims of identity-related crime appear not to have taken full advantage of existing avenues of recourse under civil law. This is not surprising, given the many obstacles and disincentives to litigation in the context of identity-related crime, which typically include:

- Inability to identify the perpetrator and/or organization(s) that facilitated the crime;
- Inability to prove a causal connection between organizational negligence and losses suffered;
- The unpredictability of litigation with respect to both findings and remedies;
- The exorbitant cost of litigation, including the costs associated with gathering evidence;
- The likelihood of a low damage award if successful;
- The low likelihood of being able to collect from the perpetrator any damages awarded;
- The necessary public exposure of one’s private affairs; and
- The emotional burden of litigation.

As stated in a recent report on the rights of identity theft victims in Australasia, “The major deterrent to such actions being initiated is the potential legal and expert witness costs involved—not only the plaintiff’s costs, but also the defendant’s costs if the action is unsuccessful. In addition, individuals initiating action may be required by the court (before the matter is heard) to provide undertakings or security as to costs in the event of the action being unsuccessful.”<sup>104</sup>

## 4. Relevant human rights

Certain human rights recognized in international and domestic law may be relevant to, and may even create legal duties for, State measures to remediate victims of identity-related crime. These include rights to identity, reputation and privacy, each of which is discussed below.

<sup>103</sup> Jennifer Chandler, “Negligence Liability for Breaches of Data Security”, 23 *Banking & Finance Law Review* (2008), pages 223-247.

<sup>104</sup> Blindell, (2006).

### *Application of international and constitutional human rights to private sector relations*

Constitutional rights are typically limited in direct application to the public sector, and apply only indirectly to the private sector through their application to legislation affecting private bodies, and through their status as established higher norms that infuse and guide the interpretation of law governing private relations. Courts have for the most part been reluctant to extend public sector human rights so as to find public sector duties vis-à-vis matters in the private sphere (such as a duty to remediate victims of crime). Constitutionally guaranteed rights can, however, provide a basis upon which public sector duties to protect citizens from private sector wrongdoing may be found.<sup>105</sup> In some jurisdictions, constitutional rights may apply directly to the private sector.<sup>106</sup>

Apart from explicit provisions extending constitutional protections to the private sector, the application of constitutional rights to the private sector is most notably found in the European doctrine of “*drittwirkung*”, under which fundamental human rights set out in constitutional documents can form the basis of rights and duties between private actors. Although this doctrine remains the subject of debate, it has been applied in a number of cases. For example, the European Court of Human Rights has found that Article 8 of the European Convention on Human Rights (“ECHR”)<sup>107</sup> can apply to privacy violations between private parties so as to require the adoption of protective measures (e.g., additional criminal laws) by the state where existing measures (e.g., civil law) are inadequate,<sup>108</sup> stating in a recent case as follows:

42. The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see *Airey v. Ireland*, judgment of 9 October 1979, Series A No. 32, § 32).

43. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. There are different ways of ensuring respect for private life and the nature of the State’s obligation will depend on the particular aspect of private life that is at issue. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State’s margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions (see *X and Y v. the Netherlands*, §§ 23-24 and 27; *August v. the United Kingdom* (dec.), No. 36505/02, 21 January 2003 and *M.C. v. Bulgaria*, No. 39272/98, § 150, ECHR 2003-XII).

[...]

<sup>105</sup> See Dawn Oliver and Jörg Fedtke, eds, *Human Rights and the Private Sphere: A Comparative Study* (Routledge, 2007).

<sup>106</sup> For example, Article 25(1) of the Greek Constitution states: “These rights also apply to the relationship between individuals wherever appropriate.”

<sup>107</sup> i.e., The right to respect for private and family life. See below, under “Right to Privacy” for a substantive discussion of this right.

<sup>108</sup> *X and Y v. The Netherlands* (1985), ECHR Case No. 16/1983/72/110. This case involved the state’s failure to prosecute a case involving rape of a mentally incapacitated adult due to a legislative gap.



46. [...] the Court notes that it has not excluded the possibility that the State's positive obligations under Article 8 to safeguard the individual's physical or moral integrity may extend to questions relating to the effectiveness of a criminal investigation even where the criminal liability of agents of the State is not at issue (see *Osman v. the United Kingdom*, judgment of 28 October 1998, Reports 1998-VIII, § 128). For the Court, States have a positive obligation inherent in Article 8 of the Convention to criminalize offences against the person including attempts and to reinforce the deterrent effect of criminalization by applying criminal-law provisions in practice through effective investigation and prosecution (see, *mutatis mutandis*, *M.C. v. Bulgaria*, cited above, § 153).<sup>109</sup>

## Right to identity

### Nature of right

Identity is an inherent necessity of the individual. It is essential in order for the individual to establish and maintain psychological, social, and cultural ties and to participate in human groupings including family, society and nation-states. Without a recognized identity, individuals cannot participate fully in society and cannot exercise civil and political rights. Elements of identity include, among other things, attributes such as name and nationality, biometric characteristics such as fingerprints, and biographical information such as date of birth, family and employment history.

The right to civil identity (in particular, to name, nationality, registration, juridical personality) is a basis on which other political, social and economic rights (as well as obligations) flow. It generates rights to citizenship and democratic participation, to standing before state institutions and mechanisms, to state benefits and programmes including health care and education, and to private rights such as employment, property ownership, and credit.

### Legal basis

In international law, the right to identity has been treated both as an autonomous right and as an expression or element of other rights such as the right to be registered, the right to a name, the right to nationality and the right to juridical personality.<sup>110</sup> Such rights are recognized in a number of international human rights conventions and other documents, including:

- Universal Declaration of Human Rights, 1948 (Article 6: "Everyone has the right to recognition everywhere as a person before the law."; Article 15: "Everyone has the right to a nationality.");

<sup>109</sup> *K.U. v. Finland*, Appl. No. 2872/02 (2 December 2008). In this case, the court held unanimously that there had been a violation of Article 8 of the ECHR Rights concerning the Finnish authorities' failure to protect a child's right to respect for private life following an advertisement of a sexual nature being fraudulently posted in the child's name on an Internet dating site. In particular, Finland was found to have violated the applicants' right to privacy by failing to have a legislative provision permitting ISPs to identify the person who had posted the advertisement in situations such as this.

<sup>110</sup> Permanent Council of the Organization of American States, Committee on Juridical and Political Affairs, *Preliminary Thoughts on Universal Civil Registry and the Right of Identity*, OEA/Ser.G CP/CAJP-2482/07 (16 April 2007)

- American Declaration of the Rights and Duties of Man, 1948, (Article XVII. “Every person has the right to be recognized everywhere as a person having rights and obligations, and to enjoy the basic civil rights.”; Article XIX: “Every person has the right to the nationality to which he is entitled by law and to change it, if he so wishes, for the nationality of any other country that is willing to grant it to him.”);
- International Covenant on Civil and Political Rights, 1966 (Article 16: “Everyone shall have the right to recognition everywhere as a person before the law.”; Article 24.2: “Every child shall be registered immediately after birth and shall have a name.” Article 24.3: “Every child has the right to acquire a nationality.”);
- United Nations Convention on the Rights of the Child, 1989 (Article 7: “The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and as far as possible, the right to know and be cared for by his or her parents.”; Article 8: “1. States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name and family relations as recognized by law without unlawful interference. 2. Where a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection with a view to speedily re-establishing his or her identity.”).

### Application of right generally

The right to identity has been promoted in recent years as the basis for universal civil registration and national identification in certain regions in an effort to ensure that all citizens can enjoy basic rights.<sup>111</sup> In this context, it is seen as underlying the state’s duty to ensure that all citizens are registered, and to assist citizens in recovering civil identity documents lost as a result of civil war, displacement, natural disasters, and other causes.

The right to identity is also referenced in efforts to restore the identities of abducted children whose identities were altered by their abductors (especially in the context of enforced disappearance of their parents). The United Nations Declaration on the Protection of All Persons from Enforced Disappearance,<sup>112</sup> Article 20.3, addresses this issue directly as follows:

The abduction of children of parents subjected to enforced disappearance or of children born during their mother’s enforced disappearance, and the act of altering or suppressing documents attesting to their true identity, shall constitute an extremely serious offense, which shall be punished as such.

As noted above, the United Nations Convention on the Rights of the Child, Article 8, addresses identity restoration in the context of illegal deprivation of children’s identities, stating:

2. Where a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection with a view to speedily re-establishing his or her identity.

<sup>111</sup> Permanent Council of the Organization of American States, Committee on Juridical and Political Affairs, Draft Resolution: Inter-American Program for a Universal Civil Registry and “The Right to Identity”, OEA/Ser.G, CP/CAJP-2465/07 rev. 4 (15 May 2007).

<sup>112</sup> G.A.Res. 47/133, UN GAOR, 47th Session, Supp. No. 49, Article 20, United Nations Doc. A/47/49 (1992).

### Application to identity-related crime

The right to identity has not been widely promoted (if at all) as the basis for programmes and actions to assist victims of crime other than in the narrow contexts above—i.e., the creation of identity information in the first place, and the restoration of identity information in the context of (a) lost documents due to natural disasters, and (b) children whose identities were altered by their abductors.

Arguably, the same legal basis for restoration could nevertheless apply in the context of identity information that has been significantly corrupted by reason of its fraudulent use, or to adult victims of identity-related crime who have been deprived of the integrity of their legal or contractual identities as a result of the actions of identity criminals, where the State has failed to take adequate measures to protect against such fraud.

One important difference, however, is that in current applications of the right to identity, the individual “victims” either lack the identity information in question (name, nationality, citizen registration) in the first place, have lost proof of their identity, or have never known their real identities. In contrast, identity-related crime as discussed in this paper involves the misappropriation and fraudulent use of another person’s established identity information. The victim of these kinds of crimes does not “lose” his or her identity as such, and often does not even lose possession of the relevant identity information.

### *Right to privacy*

#### Nature of right

Privacy is widely acknowledged as a fundamental, but not absolute, human right, underpinning human dignity and autonomy as well as other rights such as freedom of association and expression. Privacy can be divided into different but related concepts such as:

- Territorial privacy—e.g., freedom from intrusion into one’s home or workspace;
- Bodily privacy—e.g., freedom from invasive procedures such as genetic tests, drug testing and cavity searches;
- Psychological privacy—e.g., the right to hold secrets;
- Communications privacy—e.g., the right to communicate in private; and
- Informational privacy—e.g., the right to control collection, use and disclosure of information about oneself.

The right to privacy is closely related to rights of identity and reputation. For example, the European Commission of Human Rights (created along with the European Court of Human Rights to oversee enforcement of the European Convention on Human Rights), found in 1976 that:

For numerous Anglo-Saxon and French authors, the right to respect for “private life” is the right to privacy, the right to live, as far as one wishes, protected from publicity [...]

In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality.<sup>113</sup>

### Legal basis

Privacy rights are recognized in many international and regional human rights treaties including Article 12 of the Universal Declaration of Human Rights, which states:

No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

The same language appears as Article 17 of the International Covenant on Civil and Political Rights, Article 14 of the United Nations Convention on Migrant Workers, and Article 16 of the Convention on the Rights of the Child.

Article 11 of the American Convention on Human Rights states:

1. Everyone has the right to have his honor respected and his dignity recognized.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attack.

Article 8 of the European Convention on Human Rights (ECHR) states:

Everyone has the right to respect for his private and family life, his home and his correspondence.

All European Union members are bound to this Convention, and there is a large and growing body of jurisprudence on Article 8.

Most countries in the world include a right to some form of privacy, such as the inviolability of the home and secrecy of communications, in their constitutions. The Canadian Charter of Rights and Freedoms, for example, provides for the "right to life, liberty and security of the person", as well as the right "to be free from unreasonable search and seizure", both of which have been found to include privacy rights.<sup>114</sup> Most recently written constitutions include specific rights to access and control one's personal information.<sup>115</sup>

<sup>113</sup> *X v. Iceland*, 5 Eur. Comm'n H.R. 86.87 (1976).

<sup>114</sup> Sections 7 and 8.

<sup>115</sup> EPIC et al.

Privacy rights also appear in domestic human rights legislation that does not have constitutional status, but that requires the laws of that jurisdiction to be interpreted consistently with the rights set out in the Act.<sup>116</sup>

### Applicability to identity-related crime

Identity-related crime involves direct violations of the right to privacy in a general sense. As with rights to identity and reputation, privacy rights form a strong normative basis for state action to assist victims of identity-related crime. Where they are more developed (e.g., in European and North American law), privacy rights may also create a legal basis for the adoption of effective remedial measures for victims of privacy violations such as identity-related crime.

A human rights-based argument for state action to assist victims of identity-related crime is stronger in Europe than in North America, given the existence of *drittwirkung* in Europe. In a ECHR case noted above,<sup>117</sup> the Netherlands was ordered to pay damages to a victim of sexual assault on the grounds that the protection afforded by either the criminal law or the civil law against such interference with fundamental rights was insufficient. The reasoning in this case is remarkably applicable to many identity-related crime cases, which also involve a serious violation of privacy; a need to protect against and deter such acts *erga omnes*; a failure of criminal law to clearly proscribe the particular act in question; an absence of criminal investigation; the complainant's consequent difficulty furnishing evidence to establish the wrongful act, fault, damage and a causal link between the act and the damage; and the fact that civil proceedings are lengthy and involve difficulties of an emotional nature for the victim.

### Right to reputation

Another human right relevant to identity-related crime victims is that of reputation. The right to be free from attacks on one's reputation is closely related to the right to privacy; indeed, the two are often combined in human rights instruments, including those referenced above under "Right to privacy".

Reputation rights also appear in many domestic constitutions and are often but not always linked with privacy rights. For example, Article 38 of the Chinese constitution states that the personal dignity of citizens of the People's Republic of China (PRC) is inviolable and that insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited.

As with human rights to identity and privacy, international and constitutional recognition of reputation rights offer a potential legal basis for state programmes and actions to assist victims of identity-related crime. Under the European *drittwirkung* doctrine for example, it could be argued that a State's failure to criminalize identity theft or fraud and thus to prosecute perpetrators creates State liability for victim losses, where the victim's constitutionally guaranteed right to reputation was severely damaged.

<sup>116</sup> For example, the Australian Capital Territory's Human Rights Act 2004 (s.12) and the Australian state of Victoria's Charter of Human Rights and Responsibilities.

<sup>117</sup> *X and Y v. The Netherlands*, *op cit*.

## 5. Legal framework for international cooperation in assisting victims of crime

The current framework of international, multilateral and bilateral instruments for cooperation in criminal law matters focuses on facilitating the investigation and prosecution of criminal offences and does not generally address victim issues. Mutual Legal Assistance Treaties, for example, do not usually (if at all) contemplate victim remediation. Instead, they tend to focus on cooperative measures to assist investigators and prosecutors, such as powers to summon witnesses, to compel the production of documents and other real evidence, to issue search warrants, and to serve process.

Other criminal law conventions relevant to identity-related crime are designed to establish international standards for substantive or procedural criminal law, and are similarly silent on international cooperation with respect specifically to treatment of and assistance for victims of crime. For example, while the Palermo and Merida Conventions discussed above require that State Parties take certain actions to assist victims of organized crime and corruption, respectively, their provisions for international cooperation do not explicitly apply to victim remediation. The Council of Europe Convention on Cybercrime, for its part, is explicitly designed “to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence”. It calls for Parties to cooperate with each other in such investigations and prosecutions “to the widest extent possible”, but does not address victim issues.<sup>118</sup>

However, as noted above, there is a draft United Nations Convention on Justice and Support for Victims of Crime and Abuse of Power. If adopted, it would fill this gap by providing for international cooperation not only in the investigation and prosecution of offences but also in the protection of victims “whether in the form of networks directly linked to the judicial system or of links between organizations which provide support to victims.”<sup>119</sup>

---

<sup>118</sup> Council of Europe, Convention on Cybercrime, CETS No. 185.

<sup>119</sup> Draft Convention, available online at: <http://www.tilburguniversity.nl/intervict/undeclaration/convention.pdf>.

# IV. INVENTORY OF PRACTICES FOR VICTIM REMEDIATION

The following is an inventory of measures taken by governments and private sector entities to assist and remedy the damage caused to individual victims. Such measures range from informational and educational to the establishment of enforceable victim rights and remedies. They may be voluntary or mandated by legislation, depending on the type of measure and the entity delivering it.

The inventory separates public sector and private sector practices. Most examples provided are from North America and, to a lesser extent, Europe. This reflects the information that was available to English language researchers through publicly available sources. However, it also appears to reflect a much greater attention to identity-related crime in the United States than in any other country, and possibly, a greater incidence of identity-related crime in the United States than in other countries.<sup>120</sup> Further research is needed to identify the types and incidence of identity-related crime, and relevant practices in respect of victim remediation, especially in Asia, Africa and South America.

Many of the practices listed make sense only in States with economic systems and institutional structures similar to those in the United States or other western economies (e.g., credit bureau and collection agency practices are relevant only where such organizations exist). Others assume a level of institutional resources or maturity that may not exist in all States. For this reason, the inventory is meant not as recommendations applicable to all States, but rather as a selection of noteworthy measures undertaken by certain States (and private entities in certain States) that have recognized the need to combat identity-related crime. The measures that each State chooses to adopt should reflect both the institutional and economic structure of that State and its experience with identity-related crime.

## 1. Public sector practices

Governments have the ability to assist victims of identity-related crime in a variety of different ways, both directly through State agencies and indirectly through the regulation of private sector entities. Many of the practices listed in the section entitled “Private Sector Practices” are unlikely to occur without State involvement through the enactment of legislation or enforceable codes of practice. We have nevertheless separated practices based on the entity undertaking the actual practice, whether mandated to or not. The following

<sup>120</sup> *Nicole van der Meulen*, “The Spread of Identity theft: Developments and Initiatives within the European Union”, *The Police Chief*, vol. 74, No. 5 (May 2007).

list of public sector practices therefore focuses on measures that government agencies can take to assist victims of identity-related crime. It is broken down into four categories: building institutional capacity to deal with identity-related crime, providing for victim compensation, facilitating victim self help, and preventing re-victimization.

### *Building institutional capacity to assist victims*

Governments need to build their own internal capacity to deal effectively with identity-related crime and its impact on victims. This includes developing the capacity not only to prevent and detect identity-related crime, but also to mitigate its impact on victims. Fortunately, many capacity-building practices tend to serve both purposes. Thus, many of the practices listed below may be as applicable to prevention or detection as they are to victim remediation. Governments can also assist the private sector in building its capacity to assist victims of identity-related crime. The following list includes State measures focusing on public sector and private sector capacity-building.

### **Identify and coordinate among domestic State agencies dealing with identity-related crime victims**

Because identity-related crime involves a number of different arms of government (e.g., official document issuers, service and benefits providers, law enforcement agencies), an effective state response to the problem requires coordination among the different agencies involved. This goes for victim remediation as well as for prevention purposes. Victims should be able to rectify false records and obtain new documents as necessary without undue effort.

The first step is to identify State agencies who play a role in identity-related crime, and to understand that role. Best practices can then be developed for each agency. Coordination among agencies is, however, critical if victims are to be well-served.

Best practices in this area include the United States approach, under which Congress designated the FTC as the lead agency on identity-related crime and the President appointed a high-level Task Force in 2006 to develop a coordinated approach among government agencies to combat identity crime.<sup>121</sup> Pursuant to its mandate, the Task Force issued a Strategic Plan in April 2007 with numerous recommendations for reducing the incidence and impact of identity-related crime, and a subsequent report in October 2008 on the implementation of those recommendations, many of which deal with remedial measures for victims.

Examples of specific coordinated public sector activities include:

- Establishment of a working group of prosecutors, investigators, and analysts from agencies including United States Department of Justice (“DOJ”) Criminal Division, United States Attorneys’ Offices, the FBI, the Department of the Treasury, the FTC, the Diplomatic Security Service, the United States Secret Service, and

<sup>121</sup> See website of President’s Task Force on Identity Theft: available online at: <http://www.idtheft.gov>.



the United States Postal Inspection Service that meets monthly to discuss emerging trends in identity-related crime, share best practices, and receive reports from government and private sector representatives involved in combating identity-related crime;

- Participation of the United States DOJ Office for Victims of Crime (“OVC”) in federal working groups that share information and foster collaboration in addressing issues associated with identity-related crime;
- The United States “Identity Theft Data Clearinghouse”: a national database established by the FTC that contains more than 1.6 million victim complaints about identity-related crime. Over 1,650 federal, state, and local law enforcement and regulatory authorities have access to the Clearinghouse for purposes of conducting investigations, obtaining information about identity-related crime victims, and identifying other agencies involved in an investigation;
- The United States National Identity Crimes Law Enforcement (NICLE) Network, which allows authorized law enforcement at the federal, state, and local levels to enter and retrieve identity crimes data through the Regional Information Sharing Systems Network, a centralized data sharing system. NICLE is designed to include data from the FTC, law enforcement agencies, and the banking and retail industries;
- “RECOL” (Reporting Economic Crime On-Line), a partnership among Canadian law enforcement agencies and the Internet Fraud Complaint Centre that, among other things, directs victims to appropriate agencies for investigation.<sup>122</sup>

### Coordinate with private sector on identity-related crime victim issues

Victims are frequently frustrated in their restoration attempts by the lack of coordination and information-sharing between private sector and public sector entities. Examples of useful practices and initiatives in this respect include:

- The United Kingdom “Identity Fraud Steering Committee”, a public/private partnership initiative set up by the British Home Office to coordinate existing activity on identity crime in the public and private sectors and identify new projects and initiatives to reduce identity crime;<sup>123</sup>
- Sharing by the FTC of complaint information from the Identity Theft Data Clearinghouse (described above) with private entities in order to resolve identity-related crime issues;
- Various initiatives designed to ensure that identity-related crime victims can obtain copies of records related to the crime from the businesses that dealt with the perpetrator; such initiatives include meetings between government agencies and the financial services industry, distribution of educational materials, and the establishment of an e-mail address for reporting and obtaining assistance with this particular problem;

<sup>122</sup> See: <http://www.recol.ca>.

<sup>123</sup> See: <http://www.identity-theft.org.uk/committee.asp>.

- “Identity Shield”, a public-private initiative involving the FBI’s Cyber Initiative Resource Fusion Unit (CIRFU), the National Cyber-Forensics and Training Alliance (NCFTA), the United States Postal Inspection Service, and the private sector. Under this project, CIRFU collects personal data that has been posted on the Internet by identity thieves and reports it to the major consumer reporting agencies and affected financial institutions. CIRFU and the Internet Crime Complaint Center (IC3) also work together to report the crimes to relevant law enforcement agencies;
- Establishment of Task Forces throughout the United States to aid in combating identity-related crime. These task forces are comprised of approximately 2000 state, local, private sector, and academia partners;
- The FTC’s “AvoID Theft” campaign in which businesses are invited to partner with the FTC in educating the public about identity-related crime.<sup>124</sup>

### Participate in relevant international, bilateral and regional cooperation frameworks

There are currently a number of international, bilateral and regional networks and organizations focusing on the establishment of standards and cooperative efforts to combat cross-border fraud, crime and related problems.<sup>125</sup> Increasingly, they are recognizing a need to address identity-related crime as a unique issue, given its serious impact on victims and economies generally. States can improve their capacity to assist victims of identity-related crime, as well as to prevent such crime, by sharing information and best practices and by working together to combat cross-border identity-related crime. Some such initiatives include:

- The United Nations Core Group of Experts on Identity-Related Crime (with whom this Discussion Paper was prepared), convened by the United Nations Office on Drugs and Crime pursuant to the United Nations Commission on Crime Prevention and Criminal Justice’s 2007 Resolution on International Cooperation in the Prevention, Investigation, Prosecution and Punishment of Economic Fraud and Identity-Related Crime;<sup>126</sup>
- The OECD’s development of various Guidelines, Recommendations and Toolkits for member States on such matters as security of information systems and networks, protection of privacy and transborder flows of personal data, cross-border fraud, electronic commerce, and consumer dispute resolution and redress;<sup>127</sup>
- The International Consumer Protection Enforcement Network (“ICPEN”), through which consumer protection enforcement authorities from 36 countries cooperate and share information on fraud affecting consumers, through monthly teleconferences, national reports and the econsumer.gov website;<sup>128</sup>

<sup>124</sup> See: <http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html>.

<sup>125</sup> See OECD, Directorate for Science, Technology and Industry, Committee on Consumer Policy, *Scoping Paper on Online Identity Theft*, DSTI/CP(2007)3/FINAL (19 February 2008) [“OECD”], pages 45-55, for a more comprehensive list and description of such initiatives.

<sup>126</sup> E/RES/2007/20 (26 July 2007); see also E/RES/2004/26 (21 July 2004).

<sup>127</sup> See OECD, *op cit*, pages 45-46.

<sup>128</sup> As reported in OECD, *ibid*.

- The “London Action Plan”, a global network of public and private sector parties focused on cooperating internationally to combat spam;<sup>129</sup>
- The G8 24/7 High Tech Crime Network, which includes 45 countries, facilitates the sharing of information among States on ongoing investigations against cyber-criminals, including those involving identity-related crimes.<sup>130</sup>

### Mandate a central agency to deal with identity-related crime

Victims should not have to deal with multiple agencies in order to obtain information about their rights, government services available to them, and other matters relevant to restoration. But it is also in the government’s interest to provide a central point for information on identity-related crime, for capacity-building purposes as well as for reasons of efficiency and effectiveness. A central agency will develop expertise over time and thus be more effective in dealing with this multi-faceted and often complex form of crime.

Under the United States Identity Theft and Assumption Deterrence Act 1998, which created a specific offence of “identity theft”,<sup>131</sup> the Federal Trade Commission (“FTC”) was tasked with creating a central information, assistance and complaint-referral service for victims of identity-related crime.<sup>132</sup> The FTC therefore established a service that includes the following:

- A clearinghouse for complaints about identity-related crime;
- A website with relevant information for victims;
- A hotline providing advice and counsel to victims through which data on the incidence of ID-related crime is collected;
- Referral of victim complaints to appropriate entities; and
- Outreach (particularly to state and local law enforcement agencies) and education to consumers, law enforcement, and private industry.

The FTC has therefore become the main source of information on identity-related crime in the United States and a key player in the national strategy to combat this crime. Although other government agencies play important roles (e.g., the Department of Justice’s Office for Victims of Crime, national and local law enforcement agencies), tasking the FTC with developing a centralized complaint and consumer education service for victims of identity-related crime has avoided unnecessary duplication of effort while better serving victims.

### Expand existing programmes for victims of crime to cover identity-related crime

Many States have services and programmes designed specifically to assist, support and/or compensate victims of crime. Such programmes tend to focus on victims of violent crime or other crimes fundamentally different in nature from identity-related crime, and are not

<sup>129</sup> Ibid.; a major technique used by identity criminals to gather personal data from victims is “phishing”, i.e., the use of unsolicited bulk e-mail (“spam”) to deceive individuals into providing their account and other data.

<sup>130</sup> Ibid.

<sup>131</sup> Defined broadly to include identity fraud and related acts: 18 USC. § 1028.

<sup>132</sup> Pub. L. No. 105-318 § 5, 112 Stat. 3010 (1998).

always well-equipped to assist victims of identity-related crimes even where recognized as offences under criminal law.

Some public sector offices with the mandate of assisting victims of crime do offer at least indirect assistance to victims of identity-related crime. For example, the United States Office for Victims of Crime works to raise awareness of identity-related crime's consequences for victims, has sponsored several initiatives to help victims of identity-related crime, and supports service providers, allied professionals, law enforcement, and others tasked with helping victims.<sup>133</sup>

Also, some victims' rights laws, such as New Zealand's Victim Rights Act, cover victims of identity-related crime as long as they have suffered a direct financial loss.<sup>134</sup>

### Support private sector victim support initiatives/programmes

Victim support can often be provided more effectively by non-governmental agencies devoted to the issue. In the United States, where identity-related crime appears to be most prevalent, there are a number of such organizations. In 2007, the United States government awarded \$1.7 million through its Office for Victims of Crime to existing national, regional, state and local victim service organizations for the purpose of supporting programmes that assist victims of identity-related crime.<sup>135</sup>

The United States Department of Justice is currently collaborating with the American Bar Association to set up a programme supporting lawyers who represent victims of identity-related crime free of charge.

### Provide educational materials and training for law enforcement officers and others who deal with victims of identity-related crime

Victims often turn first to the police for assistance, and are frequently met with unhelpful responses. Moreover, obtaining an official "police report" is often critical in order for victims of identity-related crime in North America to clear their names. Yet victim requests for such reports are frequently refused by police agencies. The International Association of Chiefs of Police, together with the Bank of America, has published information and a "toolkit" for law enforcement agencies in dealing with victims of identity-related crime on the website [www.idsafety.org](http://www.idsafety.org).

The FTC has created a CD-ROM exclusively for law enforcement titled *Fighting Identity Theft: A Law Enforcer's Resource* and has distributed thousands of copies to police departments across the country. The CD-ROM contains a variety of resources for law enforcement and first responders to assist victims in the recovery process, such as sample letters that can be sent to businesses requesting that they provide, without subpoena, all records related to the identity-related crime to both the victim and the investigating agency. The CD-ROM also offers advice on coordinating with other law enforcers, raising community awareness

<sup>133</sup> See: <http://www.ojp.gov/ovc/publications/infores/focuson2005/identitytheft/welcome.html>.

<sup>134</sup> Victims' Rights Act 2002 (N.Z.) 2002/39.

<sup>135</sup> See press release, available at: <http://www.ojp.usdoj.gov/newsroom/pressreleases/2007/OVC08006.htm>.

about identity-related crime, and advising local businesses about data security. It contains links to relevant laws and explains how law enforcement can access the FTC's Identity Theft Data Clearinghouse, which contains over 1.6 million searchable consumer complaints.

The United States Office for Victims of Crime runs courses specifically aimed at training law enforcement and victim assistance counsellors to manage identity-related crime.<sup>136</sup>

The FTC and other United States agencies also offer day-long identity theft seminars to law enforcement officers across the country. These seminars, which cover a wide range of topics related to identity-related crime, contain an entire segment on helping victims begin the recovery process, and stress the importance of police reports and provide access to the many victim recovery resources available to both law enforcement and victims.<sup>137</sup>

Some victims turn to lawyers for assistance. The FTC and DOJ have developed a preliminary attorney "deskbook" on identity theft, which provides *pro bono* practitioners with guidance on key legal issues arising under federal law on which identity-related crime victims may need assistance. The "deskbook" will provide tools and resources for *pro bono* attorneys to assist victims who are having difficulty clearing their credit or criminal histories.<sup>138</sup>

### *Providing for victim compensation*

#### Provide for restitution to ID crime victims in cases of criminal conviction

Victims of identity-related crime should be entitled to restitution from convicted criminals for direct and indirect losses, including the value of time spent attempting to remediate damage caused by the crime.

Under the United States Identity Theft Assumption and Deterrence Act 1998, victims of identity fraud have the right to restitution including "payment for any costs, including attorney fees, incurred by the victim (a) in clearing the credit history or credit rating of the victim; or (b) in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as a result of the actions of the defendant."<sup>139</sup> Similar amendments to the Canadian Criminal Code have been proposed to permit restitution to victims of identity crimes.<sup>140</sup>

The recently enacted United States Identity Theft Enforcement and Restitution Act provides for additional restitution to cover "the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense."<sup>141</sup> This is important given the amount of time that victims of identity-related crime typically must spend restoring their identity information and reputation.

<sup>136</sup> See, for example: <http://www.sei2003.com/ovcttac2008/SanDiego-Identitytheft.htm>, [http://www.ovcttac.gov/trainingCenter/workshop\\_descriptions.cfm#WS5](http://www.ovcttac.gov/trainingCenter/workshop_descriptions.cfm#WS5).

<sup>137</sup> The President's Identity Theft Task Force, "Combating Identity theft", vol. II, part O.

<sup>138</sup> The President's Identity Theft Task Force Report, available online at: <http://www.idtheft.gov/reports/IDTReport2008.pdf>, at page 26.

<sup>139</sup> 18 USC. 3663A(c)(1)(A).

<sup>140</sup> Bill C-27, introduced in the 39th Parliament.

<sup>141</sup> 18 USC. 3663(b).

### Apply restorative justice approaches in appropriate cases

“Restorative justice” processes may be appropriate in certain cases of identity-related crime, for example where the offender is an individual known to or located in the same community as the victim. Restorative justice is a victim-centred approach to criminal justice that is gaining popularity and is available in some jurisdictions. “A theory of justice that emphasizes repairing the harm caused or revealed by criminal behaviour”,<sup>142</sup> it requires dialog between the offender and victim, through which the offender is expected to take responsibility for his or her actions and to apologize and/or offer some kind of restitution to the victim. It will therefore only be appropriate or possible in certain cases of identity-related crime.

### Create statutory rights of action for identity-related crime victims

Victims should also be able to recover damages via the civil courts from both perpetrators (when they can be identified) and those whose negligence contributed to the damage. As noted in the section on civil law in chapter II above, there are a number of causes of action that could apply in common law jurisdictions, and a number of relevant provisions under civil law codes. However, the cost and uncertainty of civil litigation and the challenges of establishing causation in identity fraud cases serve as a strong inhibitor of such lawsuits. Statutory rights of action designed to overcome some of these obstacles could make it easier for victims to avail themselves of the civil law courts in order to obtain redress.

Several states, including California, Connecticut, Iowa, Louisiana, New Jersey and Pennsylvania, have enacted legislation creating a civil cause of action specifically for identity-related crime, some of which allows victims to recover treble damages and attorney fees.

Given the often insurmountable difficulties victims face in identifying and prosecuting identity criminals themselves, it is important that such statutory rights of action also apply to third parties whose acts or negligence facilitated the crime. In this respect, it was reported in late 2005 that the South Korean government planned to introduce legislation requiring financial institutions to compensate their customers for losses resulting from economic identity theft or fraud, unless the victims had been careless with card details, PINs and passwords. The move followed an incident in which the Korea Exchange Bank refused to compensate customers who had incurred losses from an online banking scam, saying that it would not compensate scam victims unless they could prove that the bank was at fault.<sup>143</sup>

### *Facilitating victim self-help*

### Publish information tailored to the needs of identity crime victims

Victims of identity-related crime often do not know where to turn, and are often overwhelmed by the challenges they face in restoring their reputations and identity information.

<sup>142</sup> See: <http://www.restorativejustice.org>.

<sup>143</sup> See “Korean Banks forced to compensate hacking victims”, *Finextra.com* (December 2005), available online at: <http://www.finextra.com/fullstory.asp?id=14634>.

At a minimum, governments should provide victims with the information they need to pursue restoration and redress on their own.

As part of its National Crime Prevention Programme, the Australian government released in 2004 an Identity Theft Information Kit which includes a section on “What to do if you become a victim of identity theft”, a list of identity fraud information and assistance sites, template forms for declaring the theft/fraud and related losses, and a “quick reference: checklist for both preventative and restoration purposes.”<sup>144</sup>

### Create a dedicated website on identity-related crime with information for victims

An easy and obvious best practice is to create a single national website with comprehensive information and resources for victims of identity-related crime. In the United Kingdom, public and private sector organizations have partnered to create the website [www.identity-theft.org.uk](http://www.identity-theft.org.uk), a central repository of information on identity-related crime.<sup>145</sup> Australia has also created a central website for information for victims and others on identity-related crime.<sup>146</sup> In the United States, the FTC has operated such a site for some years,<sup>147</sup> and [www.idtheft.gov](http://www.idtheft.gov) was recently created by the President’s Task Force on Identity Theft. Both sites provide a comprehensive set of information and links to various resources for victims in the United States.

The International Association of Chiefs of Police has partnered with the Bank of America to publish the website [www.idsafety.org](http://www.idsafety.org), which includes extensive information for victims, including a statement of rights and “toolkit” for victims.

### Establish a victim support centre and/or hotline

Where the provision of online information and self-help is inadequate, victims of identity-related crime should have access via a toll-free number to obtain free advice, counseling, and assistance with the process of restoring their identity information. This can be done through existing victims’ support organizations or separately.

As noted above, the FTC offers counseling to victims of identity-related crime through its hotline 1-877-ID-THEFT. Similar services are provided by a number of non-profit groups and crime victims’ organizations such as VICARS (Victims Initiative for Counseling, Advocacy and Restoration), a non-profit law office that services the Southwest United States<sup>148</sup> and general crime victim resource centres such as those in Maryland, United States,<sup>149</sup> and the Netherlands.<sup>150</sup>

<sup>144</sup> See link to “ID Theft Kit” on: [http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention\\_Identitysecurity#q3](http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity#q3).

<sup>145</sup> <http://www.identity-theft.org.uk/>.

<sup>146</sup> <http://www.stopidtheft.com.au/>.

<sup>147</sup> See: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

<sup>148</sup> For a more detailed description of their mission and services, see: <http://www.idvictim.org/AboutUs.cfm?pagename=AboutUs>.

<sup>149</sup> See: [http://www.mdcrimevictims.org/\\_pages/id\\_theft.html](http://www.mdcrimevictims.org/_pages/id_theft.html).

<sup>150</sup> See: <http://www.slachtofferhulp.nl/>.

### Publish an “Identity Crime Victim Statement of Rights”

First-time victims of identity-related crime are usually unaware not only of the steps they need to take to restore their reputations, but also of their relevant legal rights. The United States FTC publishes on its website an “Identity Theft Victims’ Statement of Rights”, summarizing victims’ rights in the United States.<sup>151</sup> This provides victims with a nice compilation of their rights, thus easing the process of restoration.

### Create a standard affidavit/complaint form for victims to use in the restoration process

Victims of identity-related crime typically have to deal with multiple organizations in order to correct records about them and restore their reputations. Each organization usually requires extensive written documentation. Establishing a common form for victims to use with multiple agencies saves victims a great deal of time and effort in the restoration process.

The FTC, together with criminal law enforcers and representatives of financial institutions, the consumer data industry, and consumer advocacy groups, have developed a universal “Identity Theft Complaint” form for use by victims. This form is designed to be incorporated into police department report systems, thereby facilitating the creation and availability of police reports (“Identity Theft Reports”) which victims in the United States need to exercise many of their rights, such as placing a 7-year fraud alert on their credit file or blocking fraudulent information from their credit reports. The form is available online at [www.idtheft.gov](http://www.idtheft.gov).

Canadian government agencies have also collaborated on a standard “Identity Theft Statement” designed to help victims notify financial institutions and other companies of the theft/fraud and to provide the information needed to start an investigation.<sup>152</sup> This form does not, however, replace agency-specific forms needed for restoration purposes.

### Provide victims with an official police report upon request

One of the biggest obstacles to victim remediation is the inability to obtain a police report, in order to have financial and other institutions take the victim’s allegations seriously. In many cases, police refuse to provide such reports unless the financial institution requests it.

In addition to educating law enforcement agencies about the importance of providing such reports, United States government agencies and victims’ rights organizations have facilitated victim access to such reports through the provision of a standard “Identity Theft Complaint Form” and sample letter to police forces.<sup>153</sup>

<sup>151</sup> For the complete list, see: <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html>.

<sup>152</sup> See: <http://www.phonebusters.com/images/IDtheftStatement.pdf>.

<sup>153</sup> See: <http://www.ftc.gov/bcp/edu/microsites/idtheft/tools.html>.



### Establish a process for correcting official records

One of the most challenging and frustrating aspects of restoration for victims of identity-related crime is correcting official records. Normal bureaucratic problems are compounded by the ironic risk that requests for new or revised foundation documents, the expungement of criminal records, or changes to other records can be easily abused by identity thieves and fraudsters. Victims nevertheless need a relatively simple, low cost, accessible process by which they can clear their names and get on with their lives.

A number of states have created a formal process for expunging a criminal record that was fraudulently generated as a result of identity theft.<sup>154</sup>

### Notify affected individuals of security breaches exposing their data to potential identity-related crime

Identity criminals can and do in some cases take advantage of security breaches exposing personal data to unauthorized access. If affected individuals are unaware of such exposures, they cannot be expected to take targeted action to prevent or mitigate fraudulent use of the identity information in question. For this reason, almost all North American states have passed security breach notification laws requiring that organizations notify individuals of breaches that expose their data to potential identity-related crime.<sup>155</sup> However, most such laws do not apply to public sector organizations.

### *Preventing re-victimization*

Identity-related crime is frequently an ongoing crime, resulting in repeated victimization often over a period of many years. Even when victims close corrupted accounts and obtain new identity information, fraudsters may continue to successfully impersonate the victim so as to open up new accounts or obtain benefits in the victim's name or evade authorities. Best practices for victim assistance therefore include measures to detect and prevent additional identity fraud once discovered.

### Establish a process for certifying that victim is a victim

Particularly in cases of criminal evasion identity fraud, when victims risk being arrested for crimes committed in their names, an extremely valuable service is state provision of an official document certifying that the individual is a victim of identity-related crime. Such documents are also very useful in the process of restoration and to assist victims authenticate themselves with creditors and document issuers.

Under the Ohio Attorney General's Identity Theft Verification Passport Program, for example, victims of identity-related crime may apply for a "Passport" after filing a police report. Using biometric and other technologies to create digital identifiers, the "Passport" helps victims identify and/or defend themselves against fraudulent criminal charges,

<sup>154</sup> See: <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-expunge.html>, which provides a list of all of the states with such a law, as well as a link to the relevant statute.

<sup>155</sup> See: <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.

restore credit, and prevent further misuse of their personal information. The programme also prevents duplicate entries of the victim's information.<sup>156</sup> A number of other North American states have since begun similar programmes.<sup>157</sup>

### Track stolen, lost, and fraudulent identity documents

By keeping track of stolen, lost and fraudulent identity documents and making this information available to organizations for authentication purposes, States can facilitate the detection of attempted identity fraud and thus protect victims from further damage.

The Netherlands, Belgium, Germany and Interpol operate databases that track stolen, lost and fraudulent identity documents for the purpose of detecting identity fraud. The Dutch database is accessible to public and private sector organizations and includes records of death so as to assist in detecting the fraudulent use of deceased persons' identities. There are hundreds of terminals from which the database can be accessed. The Belgian database permits the checking of stolen ID card numbers via the Internet. The German database, operated by the police, keeps records of lost and stolen payment cards and is accessible to merchants. Interpol's Stolen and Lost Travel Documents Database (SLTD) contains details of more than 11 million travel documents, and is only accessible to law enforcement authorities. However, Interpol's database on counterfeit payment cards (CPCD) is accessible to both public and private sectors.

### Regulate, or provide public information/warnings about, private sector fee-based victim remediation services

In the United States, a whole new industry is developing to serve victims of identity-related crime.<sup>158</sup> In some cases, victims are being re-victimized by commercial organizations attempting to cash in on growing fear about identity-related crime. While some of these services provide value to some victims, many charge significant fees for services that are free to the public and/or that offer little in the way of value to victims. Such services take advantage of victims who are unaware of their rights and who are often desperate for assistance.

The FTC has published a fact sheet for consumers on such services, entitled "To Buy or Not to Buy". More could be done to protect victims (and consumers generally) from exploitation by this burgeoning industry.

### Carefully authenticate applicants for identity documents

An obvious best practice for government agencies in preventing further victimization is to take special precautions when authenticating requests for identity documents, changes of address or other identity documentation.<sup>159</sup>

<sup>156</sup> See: <http://www.ag.state.oh.us/victim/idtheft/index.asp>.

<sup>157</sup> See: <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-passport.html>, which provides a link of the states with a passport type programme as well as links to the statutes.

<sup>158</sup> See, for example: [www.prepaidlegal.com](http://www.prepaidlegal.com), [www.trustedID.com](http://www.trustedID.com), [www.myidesite.com](http://www.myidesite.com), [www.creditfyi.com](http://www.creditfyi.com), [www.idcure.com](http://www.idcure.com), [www.identitytheft911.com](http://www.identitytheft911.com), [www.myidfix.com](http://www.myidfix.com).

<sup>159</sup> Careful authentication is a general prevention measure and so is merely mentioned here. It should be accomplished wherever possible without the collection or retention of personal data, in order to avoid creating additional vulnerabilities to identity-related crime.

## 2. Private sector practices

Private sector entities play a critical role in identity-related crime. Credit reporting agencies (also referred to as “credit bureaus”); financial institutions, service providers, retailers and others that grant credit; and collection agencies are all implicated in economic identity fraud, while employers, landlords, lawyers, utilities, postal agencies are also frequently fooled by identity criminals. In some cases, best practices are offered voluntarily by the organization. This is more likely when a Code of Conduct has been developed and pressure is exerted on businesses to comply with the Code. Where market forces provide insufficient incentive for companies to engage in best practices, legislation is required. Many of the practices listed below are mandated by legislation for this reason.

The following practices are organized by type of entity: credit reporting agencies, credit grantors and document issuers, collection agencies, Internet service providers, and all organizations holding personal data.

### *Credit reporting agencies*

Organizations that gather credit information about consumers and share it with credit grantors for the purpose of assessing risk are central players in economic identity fraud, as the information that they provide is relied upon by credit grantors and others to decide whether or not to loan money or provide services to the individual. Moreover, when victims first seek information and assistance in economic identity-related crime cases, they are usually directed to credit bureaus to find out the extent of the fraud and to begin the process of restoring their credit. Three credit bureaus dominate the industry in North America: Equifax, Experian, and TransUnion. Experian and Equifax are also active in the United Kingdom.

### Provide easily accessible, live support for victims

A significant frustration for many victims of economic identity fraud is the difficulty they experience contacting and obtaining information from credit bureaus. Although toll-free numbers are usually provided, it can be extremely difficult and time-consuming to navigate the recorded voice system and/or to reach a live person at such agencies. Credit bureaus can and should do a much better job making themselves available to victims. In the United States, TransUnion offers a special toll-free number for placing credit freezes, credit monitoring, and credit report, which is a step in the right direction.<sup>160</sup>

### Provide a written summary of rights to victims

Victims are typically unaware of their rights when they first discover the fraud, and if it is financial, they are usually directed first to credit bureaus to repair the damage. Credit bureaus should therefore provide a summary of rights relevant to identity fraud victims, both generally on their websites and in response to victim queries.

<sup>160</sup> See: <http://www.transunion.com/corporate/personal/consumerSupport/contactUs.page>.

Under the Fair Credit Reporting Act (“FCRA”), credit bureaus in the United States must provide identity-related crime victims with a specific FTC-approved victims’ statement of rights under credit reporting legislation.<sup>161</sup> This is in addition to the general statement of consumer rights that credit bureaus must provide.

### Offer “credit freezes” to all consumers

Victims of economic identity fraud often find themselves unable to access credit when inaccurate information about them is conveyed to potential creditors by credit reporting agencies. A “credit freeze” restricts access to the individual’s credit report, so that potential creditors and others cannot access it without the individual lifting the freeze. Because companies usually check credit reports before issuing credit, a freeze will make it unlikely that identity criminals can open new accounts in a victim’s name.

Credit freezes are perhaps the most useful tool for victims of economic identity fraud (as well as for those who simply wish to prevent identity fraud). They should be free of charge, applied for a period of time requested by the consumer, and lifted only with notice to the consumer.

Most North American states have laws requiring that credit bureaus offer credit freezes to victims of identity-related crime or to consumers generally. In the remaining states, credit bureaus offer freezes voluntarily. The cost and terms of credit freezes vary by state, but are free for victims of identity-related crime in almost all states.<sup>162</sup>

In the absence of credit freeze, credit reporting agencies should at a minimum block the reporting of allegedly fraudulent credit information. Under the FCRA, credit bureaus in the United States must immediately block the reporting of any information in the file of a consumer that the consumer identifies as resulting from an alleged identity theft or fraud, upon proof of identity and related documentation from the victim.<sup>163</sup> The bureaus must also notify the furnishers of such information that it may be fraudulent.

### Put “fraud alerts” on credit files upon request by consumers

A “fraud alert” is a notice placed on one’s credit file alerting potential creditors to the possibility that the consumer is a victim of fraud. While not as protective as credit freezes, fraud alerts can help to prevent further victimization if they are respected by credit grantors. Credit reporting agencies should make fraud alerts available to victims of economic identity-related crime free of charge.

All three major credit bureaus in North America offer fraud alerts free of charge. In some jurisdictions, they are required to do so by law while in others the practice is voluntary.<sup>164</sup>

<sup>161</sup> 15 USC. 1681g) [“FCRA”], s.609(d).

<sup>162</sup> See: [http://www.consumersunion.org/campaigns/learn\\_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html).

<sup>163</sup> FCRA, s.605B.

<sup>164</sup> Under the FCRA, all North American states must offer fraud alerts free of charge. In Canada, fraud alerts are provided voluntarily, except in the province of Ontario where they are required under the Consumer Reporting Act, R.S.O. 1990, c.C-33, s.12.1.

Under United States law, the fraud alert is initially effective for 90 days, but may be extended upon request for 7 years if the consumer provides a police report to the credit bureaus that indicates they are a victim of identity-related crime.

### Provide free credit monitoring services to victims of identity-related crime

Identity-related crime victims need access to their credit reports in order to be able to detect fraudulent use of their identity data.

Credit bureaus in the United States offer credit monitoring services for a fee, and charge for online access to credit reports. Such services should be free to victims of identity-related crime. In Canada and the United States, consumers have a right to one free copy of their credit report annually.<sup>165</sup> In addition, the FCRA gives American identity-related crime victims the right to an additional free copy of their credit report when they initially place a fraud alert, and two free copies of their report during the 12-month period after an extended (seven year) alert has been placed.<sup>166</sup>

### Coordinate victim responses with other credit bureaus; provide one-call fraud alerts

In many jurisdictions, more than one agency engages in credit reporting. As a result, victims of economic identity-related crime must deal with multiple agencies in order to clear their credit records. There is no reason why such agencies cannot coordinate so as to reduce the effort required by victims to restore their credit records.

The FCRA requires that credit bureaus “develop and maintain procedures for the referral to each other such agency of any consumer complaint received by the agency alleging identity theft, or requesting a fraud alert under section 605A or a block under section 605B.”<sup>167</sup> Under s.605A, the FCRA requires that a credit bureau that receives a request for a fraud alert contact the other two, who must add it to their files as well.<sup>168</sup> This ‘joint fraud alert’ eliminates the need for victims to contact each of the agencies separately. The same practice can and should be extended to request for credit freezes.

### *Credit grantors and document issuers*

Organizations that grant credit and issue identity documents play a critical role in identity-related crime. They can prevent damage to victims by taking measures to detect and prevent identity fraud from happening in the first place (e.g., by confirming changes of address with account holders and by carefully authenticating all applicants). Where identity fraud has already occurred, they can assist victims in mitigating damage in a number of ways.

<sup>165</sup> FCRA, s.612. See provincial credit reporting legislation in Canada, such as the Ontario Consumer Reporting Act, *op cit*.

<sup>166</sup> FCRA, s.612.

<sup>167</sup> FCRA, 15 USC. 1681s), s.621(f).

<sup>168</sup> FCRA, s.605A.

### Notify consumer if fraudulent activity suspected

Credit card companies monitor activity on cardholder accounts in order to detect abnormal patterns that could result from fraudulent use of the card. When fraud is suspected, they contact the cardholder to determine whether the activity is fraudulent. The same should be done with respect to other kinds of accounts that are known to be targeted by identity criminals.

### Cease sending inaccurate information to credit bureaus once notified of the alleged fraud

The FCRA also gives victims of identity-related crime the right to have creditors cease providing information from fraudulent transactions to consumer reporting agencies, upon provision by the victim of an “Identity theft report” with specific information.<sup>169</sup>

### Stop debt collection if notified that debt was incurred through identity-related crime

If provided with notice, along with supporting documentation such as a police report, that a debt was fraudulently incurred using the consumer’s personal data, creditors should not place the debt for collection or should remove it from collection.

### Conduct thorough authentication of all applicants for credit

Much identity fraud could be prevented, and victims thus protected from additional fraud, if organizations took more care authenticating applicants before extending credit, services, or other benefits to them. Thorough authentication is especially important with respect to individuals who have already been targeted by identity criminals.

Legislation requiring that credit bureaus offer fraud alerts also typically requires that creditors contact the consumer to confirm the transaction or take extra steps to authenticate a credit applicant before advancing credit when a fraud alert appears on the applicant’s file.<sup>170</sup>

### Provide information about the transactions in question to victims

For victims, obtaining copies of the imposter’s account application and transactions is an important step toward restoring their financial health. Under the FCRA, identity-related crime victims in the United States have a right, upon proof of their identity, to obtain copies of records related to the crime (e.g., credit applications, transaction records) from businesses that dealt with the thief, and to designate law enforcement agencies to receive this information on their behalf.<sup>171</sup>

<sup>169</sup> FCRA, s.623(a).

<sup>170</sup> FCRA s.605A; Ontario Consumer Reporting Act. S.12.3.

<sup>171</sup> FCRA, s.609(e).

### Do not hold consumers liable for fraudulent transactions beyond their control

Credit card companies typically offer limited or zero liability services to cardholders, as long as suspected fraud is reported promptly. This is a requirement under the United States Fair Credit Billing Act,<sup>172</sup> but is a voluntary practice in some other jurisdictions.

Other forms of electronic payment such as debit cards and online banking do not typically carry such liability protection for consumers. However, voluntary Codes of Conduct for Electronic Funds Transfer in Canada, Australia, and the United Kingdom limit consumer liability in the case of fraudulent transactions when the consumer has acted responsibly.<sup>173</sup>

### *Collection agencies*

In a many States, debt collection is handled mainly by private companies (“collection agencies”) hired by creditors. Victims of identity-related crime frequently only find out about the fraud when they receive a call from a collection agency seeking to collect a debt of which the victim knows nothing. A common complaint of victims is that such agencies continue to harass them for debts that they did not incur. Collection agencies can reduce the harm caused to victims of identity-related crime, while still fulfilling their obligations to creditors, in a couple of ways:

### Report alleged ID-related crime to creditors upon notification by the victim

Under the FCRA, upon notice by a victim that information related to the debt may be fraudulent or the result of identity-related crime, debt collectors must notify the creditors on whose behalf they are acting of that this may be the case.<sup>174</sup>

### Provide information about alleged debt to victim

The FCRA also requires that debt collectors who are advised that the debt is based on fraud or identity theft provide, upon request by the consumer, information about the alleged debt.<sup>175</sup>

### *All organizations holding personal data*

In addition to best practices for prevention of identity-related crime, all organizations that hold personal data can and should adopt practices to assist victims, especially in situations when the organization itself may have contributed to the risk of identity-related crime.

<sup>172</sup> 15 USC. 1693g.

<sup>173</sup> Canadian Code of Practice for Consumer Debit Card Transactions (revised 2004); Australian Electronic Funds Transfer Code of Conduct; The Banking Code (British Bankers’ Association; March 2008), each of which has been adopted by major financial institutions in the respective State.

<sup>174</sup> FCRA, s.615.

<sup>175</sup> Ibid.

## Have a policy in place to ensure timely and effective mitigation of security breaches

With the dramatic growth of computer databases containing personal information and the trade in such information, individuals are more at risk than ever of having their personal data exposed to identity criminals through security breaches. Indeed, management of security breaches has become a major issue in the United States, where the reported incidence of breaches continues to rise.<sup>176</sup> Organizations should have a clear, detailed policy in place to deal with such breaches when they happen, including measures to limit the vulnerability of exposed data to unauthorized acquisition and fraudulent use, and to assist potential victims in mitigating harm from identity-related crime facilitated by the breach.

## Notify affected individuals of security breaches

Victims of identity-related crime are often unaware of the fact until a great deal of damage has already been done to them. When organizations are aware of a heightened potential for identity-related crime as a result of their own negligence or oversight, it makes sense that they notify potentially affected individuals of such heightened risk. Most North American states have passed security breach notification laws requiring that organizations notify individuals of breaches that expose their data to potential identity-related crime.<sup>177</sup> In Japan, financial institutions are under an obligation to report data leaks to the authorities, and the Japanese Cabinet Office has issued a “Basic Policy on the Protection of Information” stating that organizations suffering data breaches should make public that fact in order to prevent secondary damage.<sup>178</sup> In Canada, Privacy Commissioners have published Guidelines for organizations responding to security breaches,<sup>179</sup> and the Australian Privacy Commissioner has issued a draft Voluntary Information Security Breach Notification Guide.<sup>180</sup> The EU is considering amendments to the Directive on Privacy and Electronic Communications (applicable to telecommunications service providers) that would introduce a data breach notification requirement.<sup>181</sup>

## Provide identity restoration services to employees or customers

A number of services for victims or potential victims of identity-related crime are now offered by a wide range of private companies in the United States. Such services include identity theft/fraud insurance; credit monitoring, control, and repair services; and general identity restoration services. While some of these services offer little of value to victims, others provide worthwhile services beyond those already available to victims free of charge.

<sup>176</sup> For a listing of data breaches, see: <http://datalossdb.org/> (global) and <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (United States).

<sup>177</sup> See: <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.

<sup>178</sup> OECD, *op cit*, pp.40–41.

<sup>179</sup> See: [http://www.privcom.gc.ca/information/guide/index\\_e.asp](http://www.privcom.gc.ca/information/guide/index_e.asp).

<sup>180</sup> See: [http://www.privacy.gov.au/publications/breach\\_0408.html](http://www.privacy.gov.au/publications/breach_0408.html).

<sup>181</sup> *Nicole van der Meulen*, “Year of Preventing Identity Crime: Moving Forward? Identity-related crime in the European Arena”, *The Police Chief*, vol. LXXV, No. 8 (August 2008).




Some employers provide identity theft/fraud insurance to their employees as part of their benefits package.<sup>182</sup> Alternatively, employers may cover the cost of an identity restoration service for employees who are victimized.

Organizations whose security breach has exposed personal data to potential identity-related crime frequently offer credit monitoring services to affected individuals.

---

<sup>182</sup> PrePaid Legal Services Inc. and Kroll are two companies that offer such products to employers. See: <http://www.prepaidlegal.com/> and [http://www.kroll.com/services/fraud\\_solutions/](http://www.kroll.com/services/fraud_solutions/).



A magnifying glass is positioned over a fingerprint, which is being scanned. In the background, a credit card is visible, showing the name 'JAMES J. SMITH', the number '0324 3954', and the expiration date '07/09'. The card also has 'VALID THRU' and 'BLADE MEMBER' printed on it.

# IDENTITY THEFT: AN INVENTORY OF BEST PRACTICES ON PUBLIC- PRIVATE PARTNERSHIPS TO PREVENT ECONOMIC FRAUD AND IDENTITY- RELATED CRIME\*

**Cormac Callanan**

**Managing Director, Aconite Internet Solutions Limited**

---

\*The present study was prepared for use as working document at the fourth meeting of the core group of experts on identity-related crime, held in Vienna, Austria, on 18-22 January 2010. It was also submitted as a Conference Room Paper to the Commission on Crime Prevention and Criminal Justice at its nineteenth session, held in Vienna on 17-21 May 2010 (E/CN.15/2010/CRP.4). The opinions expressed in this paper are those of the author and do not reflect the views of the United Nations.



# Contents

	<i>Page</i>
I. BACKGROUND .....	173
1. Identity theft .....	173
2. Threat landscape .....	174
3. Statistical context .....	176
4. 2009 statistics.....	178
5. How is your identity data stolen?.....	179
6. Online threats and globalization .....	180
II. SCOPE OF THIS STUDY .....	185
1. Purpose.....	185
2. Background of the Study .....	185
3. Purpose of the Study and specific issues to be covered.....	186
III. PUBLIC-PRIVATE PARTNERSHIPS.....	187
1. Introduction.....	187
2. The benefits of public-private partnerships .....	188
3. Raising awareness for fundamental principles of cooperation .....	189
4. Overcoming national and regional differences .....	189
5. Developing the foundation for a cooperation.....	189
6. Key indicators for successful public-private partnerships .....	190
IV. PREVENTING IDENTITY THEFT .....	191
1. Introduction.....	191
2. Awareness raising .....	192
3. Security reports .....	193
4. End-user training.....	195
5. Policy development.....	195
V. SUPPORTING INVESTIGATIONS INTO IDENTITY THEFT.....	205
1. Detecting crime and collecting evidence .....	205
2. Investigation.....	208
3. LEA training .....	210

VI. LIMITS OF COOPERATION .....	225
1. Legal limitations .....	225
2. International restrictions .....	228
3. Limits on capabilities .....	228
VII. CONCLUSION.....	231
1. What works .....	231
2. What doesn't work.....	231
3. What will happen next .....	232

# I. BACKGROUND

## 1. Identity theft

Recent studies<sup>1</sup> commissioned by UNODC in the area of identity theft indicate the necessity for public-private partnerships in combating this cybercrime activity.

As Gercke stated at the Conference on Identity Fraud and Theft,<sup>2</sup> a consistent definition of identity theft is very hard to find. Most definitions consider the term to include the subsequent fraud conducted using the stolen identity and ignore the standalone act of stealing the identity in the first place. For example, the United States Department of Justice defines identity theft and identity fraud as terms which are used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore their reputation in the community and correcting erroneous information for which the criminal is responsible.<sup>3</sup>

Javelin Research<sup>4</sup> argues that, "while the term 'identity theft' is an all-encompassing term that is widely referenced by most media, government and non-profit consumer groups on this topic, it is important to distinguish between the exposure of personal information versus the actual misuse of information for financial gain".

According to Javelin Research, identity theft happens when personal information is accessed by someone else without explicit permission. Identity fraud occurs when criminals take that illegally obtained personal information and misuse it for financial gain, by making fraudulent purchases or withdrawals, creating false accounts or attempting to obtain services such as employment or healthcare. Personally identifying information such as a Social Security number, bank or credit card account numbers, passwords, telephone calling card number, birth date, name, address, and so on, can be used by criminals to profit at the victims expense."

Gercke refers to the "different technical as well as legal measures have been developed to prevent identity theft. Such measures range from a restriction of the publication of critical

<sup>1</sup> *Dr Marco Gercke Legal Approaches to Criminalize Identity Theft for the UNODC (E/CN.15/2009/CRP.13); Philippa Lawson Identity-Related Crime Victim Issues: A Discussion Paper (E/CN.15/2009/CRP.14).*

<sup>2</sup> Conference on Identity Fraud and Theft, Tomar, Portugal, 7-9 November 2007, Internet-Related Identity Theft—A Discussion Paper.

<sup>3</sup> See: <http://www.justice.gov/criminal/fraud/websites/idtheft.html>.

<sup>4</sup> Javelin Research 2009 Identity Fraud Survey Report: Consumer Version, *Prevent—Detect—Resolve*, February 2009, <http://www.javelinstrategy.com/products/CEDDA7/127/delivery.pdf> (last visited 8 January 2010).

identity-related information to data breach notification requirements and a better protection of large databases”.<sup>5</sup>

Lawson writes about “facilitating victim self-help including publishing information tailored to the needs of identity crime victims. Victims of identity-related crime often do not know where to turn, and are often overwhelmed by the challenges they face in restoring their reputations and identity information. At a minimum, governments should provide victims with the information they need to pursue restoration and redress on their own”.<sup>6</sup>

The EC Conference on Public-Private Dialogue to Fight Online Illegal Activities on 27 November 2009 in Brussels was organized with the aim of setting up an informal platform for dialogue where different issues and topics related to the fight against online illegal activities could be discussed among private and public stakeholders as well as NGO-operated complaint hotlines. The creation of such a platform for dialogue builds upon the Council conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime.

Analysis<sup>7</sup> of systematic structures of cooperation between law enforcement agencies and Internet service providers shows that it is bidirectional in nature:

- Law enforcement agencies are, on the one hand, responsible for the prevention and investigation of crime, and on the other hand, knowledgeable about cybercrime trends;
- Internet industries are, on the one hand, victims of crime, and on the other hand, knowledgeable about cybercrime trends and hold data about their customers who are perpetrators or victims of criminal acts.

In general terms, the Internet industry and law enforcement agencies (LEAs) recognize a common interest in the prevention, detection and investigation of cybercrime and threats to national security and information infrastructure generally. Online safety, security and reliability on the Internet are dependant upon early detection of the criminal activity that might undermine the achievement of these objectives. However, this requires effective legislation which balances investigation instruments and fundamental rights, such as the right of individuals to privacy of communications and the right of individuals to be protected against criminal activities.

## 2. Threat landscape

To develop fraud prevention measures, it is essential to understand the changing nature of the threat landscape. We need to understand which type of frauds are being committed, where the victims live and where the perpetrators operate from.

<sup>5</sup> Legal Approaches to Criminalize Identity Theft, *supra* n. 1.

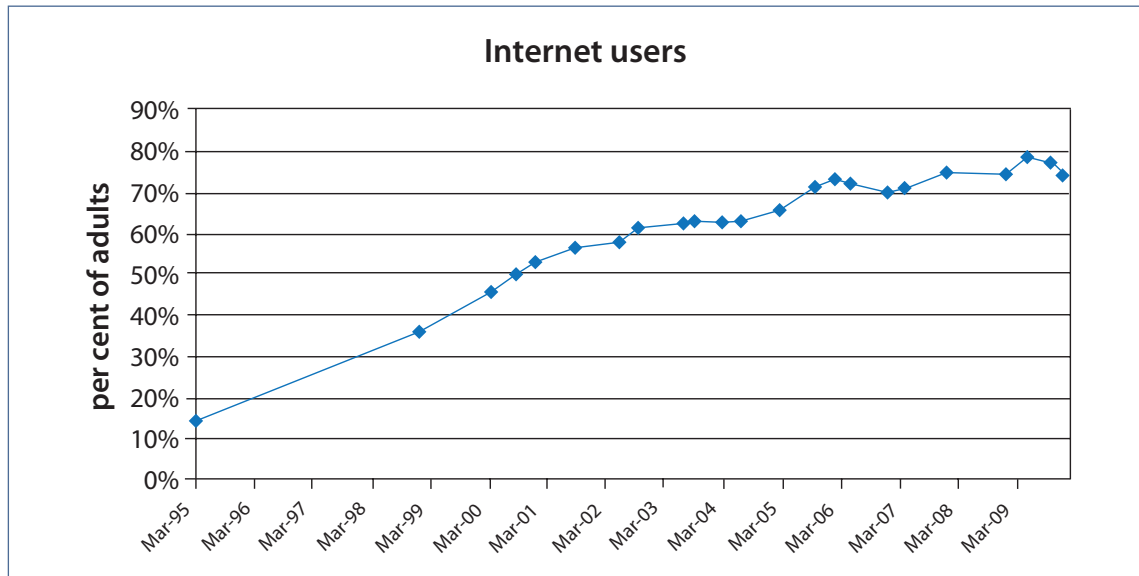
<sup>6</sup> Identity-Related Crime Victim Issues..., *supra* n. 1.

<sup>7</sup> Cooperation between service providers and law enforcement against cybercrime—towards common best-of-breed guidelines? Council of Europe, March 2008.



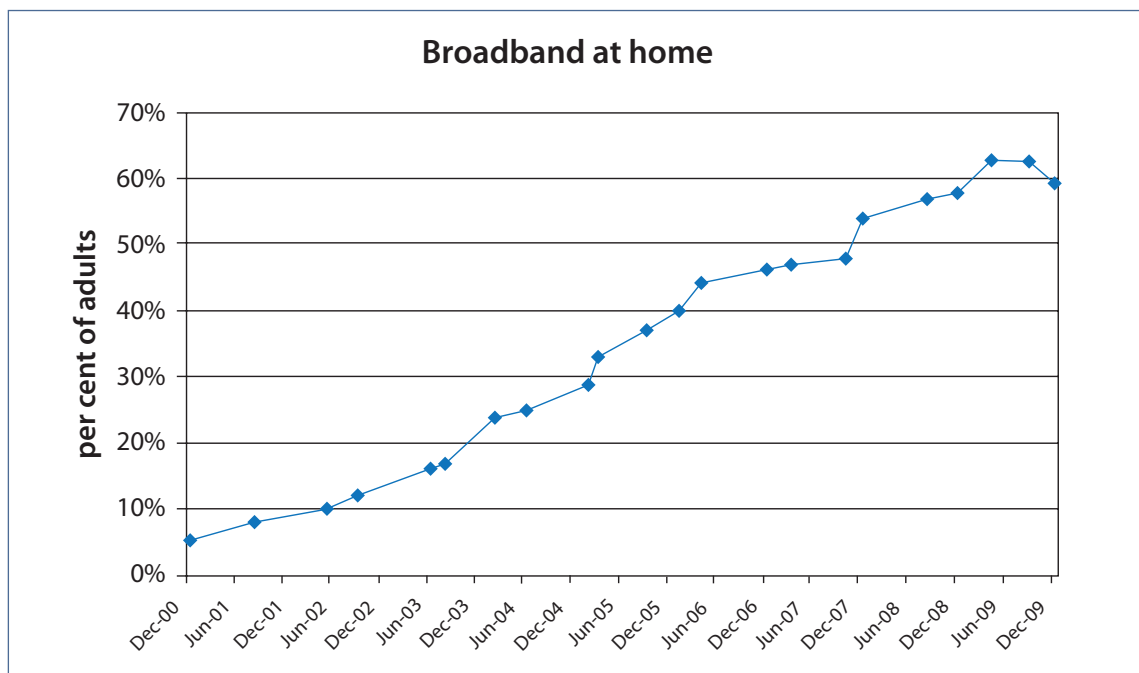
The number of users on the Internet continues to grow which can be clearly seen by research conducted for the Pew Internet & American Life Project.<sup>8</sup>

Figure 1. Online adults in the United States



Broadband at home has grown from less than 10 per cent in 2001 to over 60 per cent in 2009.

Figure 2. Broadband at home in the United States



<sup>8</sup> Internet User Profiles Reloaded, Updated Demographics for Internet, Broadband and Wireless Users, 5 January 2010, <http://pewresearch.org/pubs/1454/demographic-profiles-internet-broadband-cell-phone-wireless-users> (last visited 8 January 2010).

### 3 Statistical context<sup>9</sup>

A volume of research has been conducted on the nature of identity theft. Spendonlife.com has collated a range of very useful and interesting statistics highlighting the range of crime and the level of growth. Some of these were identified by the Javelin Research Centre.<sup>10</sup>

#### *Victims*

- There were 10 million victims of identity theft in 2008 in the United States (Javelin Strategy and Research, 2009).
- One in every ten United States consumers has already been victimized by identity theft (Javelin Strategy and Research, 2009).
- 1.6 million households experienced fraud not related to credit cards (i.e. their bank accounts or debit cards were compromised) (United States Department of Justice, 2005).
- Those households with incomes higher than \$70,000 were twice as likely to experience identity theft than those with incomes under \$50,000 (United States Department of Justice, 2005).
- Seven per cent of identity theft victims had their information stolen to commit medical identity theft.

#### *Discovery*

- 38-48 per cent discover someone has stolen their identity within three months, while 9-18 per cent of victims don't learn that their identity has been stolen for four or more years (Identity Theft Resource Center Aftermath Study, 2004).
- 50.2 million Americans were using a credit monitoring service as of September 2008 (Javelin Strategy and Research, 2009).
- 44 per cent of consumers view their credit reports using AnnualCreditReport.com. One in seven consumers receive their credit report via a credit monitoring service. (Javelin Strategy and Research, 2009).

#### *Recovery*

- It can take up to 5,840 hours (the equivalent of working a full-time job for two years) to correct the damage from ID theft, depending on the severity of the case (ITRC Aftermath Study, 2004).
- The average victim spends 330 hours repairing the damage (ITRC Aftermath Study, 2004).
- It takes 26-32 per cent of victims between 4 and 6 months to straighten out problems caused by identity theft; 11-23 per cent of victims spend 7 months to a year resolving their cases (ITRC Aftermath Study, 2004).

<sup>9</sup> <http://www.spendonlife.com/guide/identity-theft-statistics>.

<sup>10</sup> <http://www.javelinstrategy.com/>.

- 25.9 million Americans carry identity theft insurance (as of September 2008, from Javelin Strategy and Research, 2009).
- After suffering identity theft, 46 per cent of victims installed antivirus, anti-spyware, or a firewall on their computer, 23 per cent switched their primary bank or credit union, and 22 per cent switched credit card companies (Javelin Strategy and Research, 2009).
- Victims of ID theft must contact multiple agencies to resolve the fraud: 66 per cent interact with financial institutions; 40 per cent contact credit bureaus; 35 per cent seek help from law enforcement; 22 per cent deal with debt collectors; 20 per cent work with identity theft assistant services; 13 per cent contact the Federal Trade Commission (Javelin Strategy and Research, 2009).

### *Costs*

- In 2008, existing account fraud in the United States totalled \$31 billion (Javelin Strategy and Research, 2009).
- Businesses across the world lose \$221 billion a year due to identity theft (Aberdeen Group).
- On average, victims lose between \$851 and \$1,378 out-of-pocket trying to resolve identity theft (ITRC Aftermath Study, 2004).
- The mean cost per victim is \$500 (Javelin Strategy and Research, 2009).
- 47 per cent of victims encounter problems qualifying for a new loan (ITRC Aftermath Study, 2004).
- 70 per cent of victims have difficulty removing negative information resulting from identity theft from their credit reports (ITRC Aftermath Study, 2004).
- Dollar amount lost per household averaged \$1,620 (United States Department of Justice, 2005).

### *Perpetrators*

- 43 per cent of victims knew the perpetrator (ITRC Aftermath Study, 2004).
- In cases of child identity theft, the most common perpetrator is the child's parent (ITRC Aftermath Study, 2004).

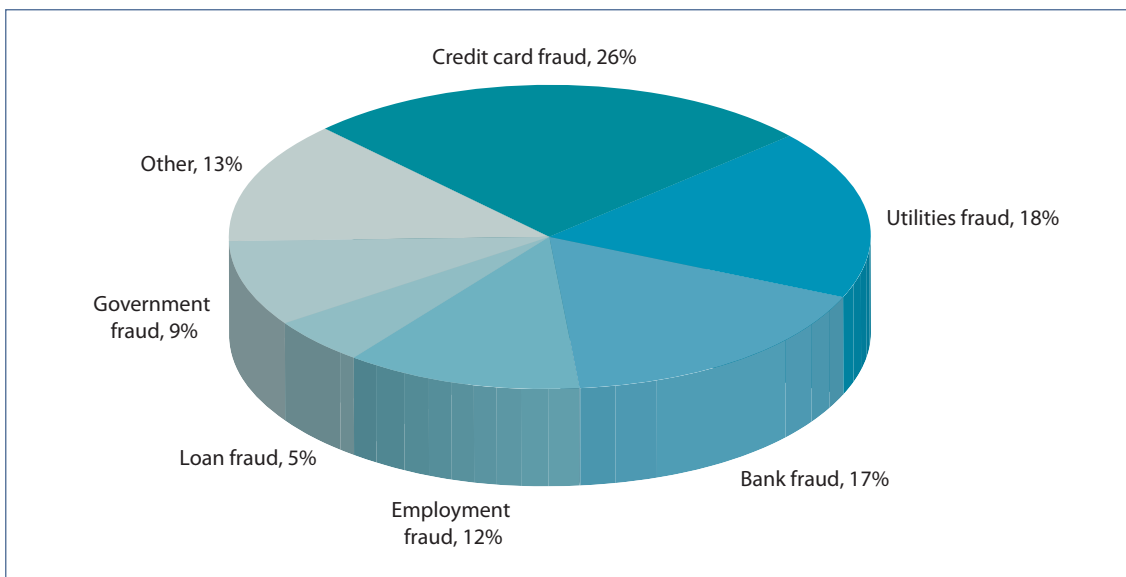
### *Methods*

- Stolen wallets and physical paperwork accounts for almost half (43 per cent) of all identity theft (Javelin Strategy and Research, 2009).
- Online methods accounted for only 11 per cent (Javelin Strategy and Research, 2009).
- 38 per cent of ID theft victims had their debit or credit card number stolen (Javelin Strategy and Research, 2009).

- 37 per cent of ID theft victims had their Social Security number stolen (Javelin Strategy and Research, 2009).
- 36 per cent of ID theft victims had their name and phone number compromised (Javelin Strategy and Research, 2009).
- 24 per cent of ID theft victims had their financial account numbers compromised (Javelin Strategy and Research, 2009).
- More than 35 million data records were compromised in corporate and government data breaches in 2008 (ITRC).
- 59 per cent of new account fraud that occurred in 2008 involved opening up new credit card and store-branded credit card accounts (Javelin Strategy and Research, 2009).

## 4. 2009 statistics

Figure 3. Range of identity fraud today



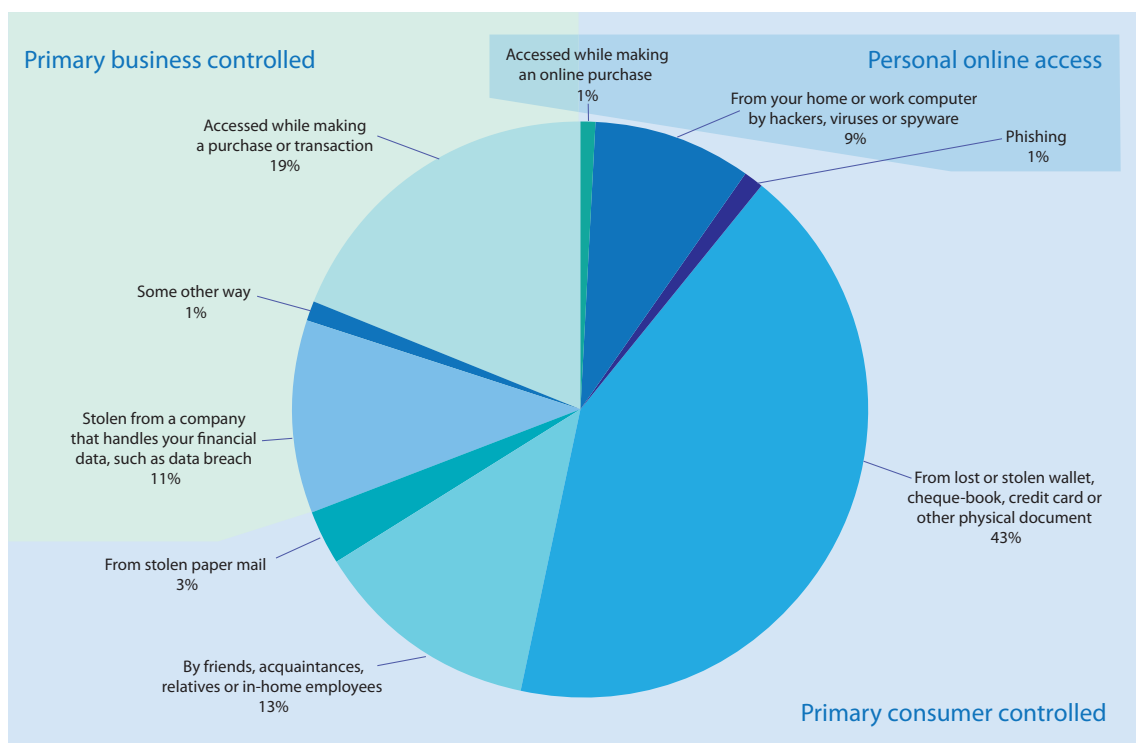
- *Credit card fraud* (26 per cent)  
Credit card fraud can occur when someone acquires your credit card number and uses it to make a purchase.
- *Utilities fraud* (18 per cent)  
Utility accounts are opened using the name of a child or someone who does not live at the residence. Parents desperate for water, gas and electricity will use their child's clean credit report to be approved for utilities.
- *Bank fraud* (17 per cent)  
There are many forms of bank fraud, including cheque theft, changing the amount on a cheque and ATM pass code theft.

- *Employment fraud* (12 per cent)  
Employment fraud occurs when someone without a valid Social Security number borrows someone else's to obtain a job.
- *Loan fraud* (5 per cent)  
Loan fraud occurs when someone applies for a loan in another name. This can occur even if the Social Security number does not match the name exactly.
- *Government fraud* (9 per cent)  
This type of fraud includes tax, Social Security, and driver license fraud.
- *Other* (13 per cent)

## 5. How is your identity data stolen?

Due to the high volume of media coverage relating to online scams—particularly the so-called Nigerian 419 scam—many users believe that the Internet is the cause of most identity theft and fraud via online hacking, phishing or malware. However, cases of fraud committed online only accounted for 11 per cent of fraud cases in 2008.<sup>11</sup> Most known cases of fraud occur through traditional methods, when a criminal has direct, physical access to the victim's information. These instances include stolen and lost wallets, cheque-books, or credit cards, or even by a criminal eavesdropping on a conversation as a purchase is made (“shoulder surfing”).

Figure 4. Most common methods of identity theft



<sup>11</sup> Javelin Strategy and Research, 2009 Identity Fraud Survey Report: Consumer Version, *Prevent—Detect—Resolve*. February 2009, page 7. <http://www.javelinstrategy.com/products/CEDDA7/127/delivery.pdf> (last visited 9 January 2010).

Indeed, there were more victims of identity theft from friends, family or in-home employees, when such data is taken without permission. Since these persons know buying habits and supervision strategies, they have better information to cover their tracks for longer periods of time.

## 6. Online threats and globalization

The global threat landscape is evolving, with malware and potentially unwanted software becoming more regional. Extremely varying threat patterns are emerging in different locations around the world. Despite the global nature of the Internet, there are significant differences in the types of threat that affect users in different parts of the world.

According to Microsoft, the malware ecosystem has moved away from highly visible threats, such as self-replicating worms, towards less visible threats that rely more on social engineering. This shift means that the spread and effectiveness of malware have become more dependent on language and cultural factors. Some threats are spread using techniques that target people who speak a particular language or who use services that are local to a particular geographic region. Others target vulnerabilities or operating system configurations and applications that are unequally distributed around the globe. As a result, security researchers face a threat landscape that is much more complex than a simple examination of the biggest threats worldwide would suggest.

The 25 locations with the most computers cleaned by Microsoft desktop anti-malware products in 1H09 were:<sup>12</sup>

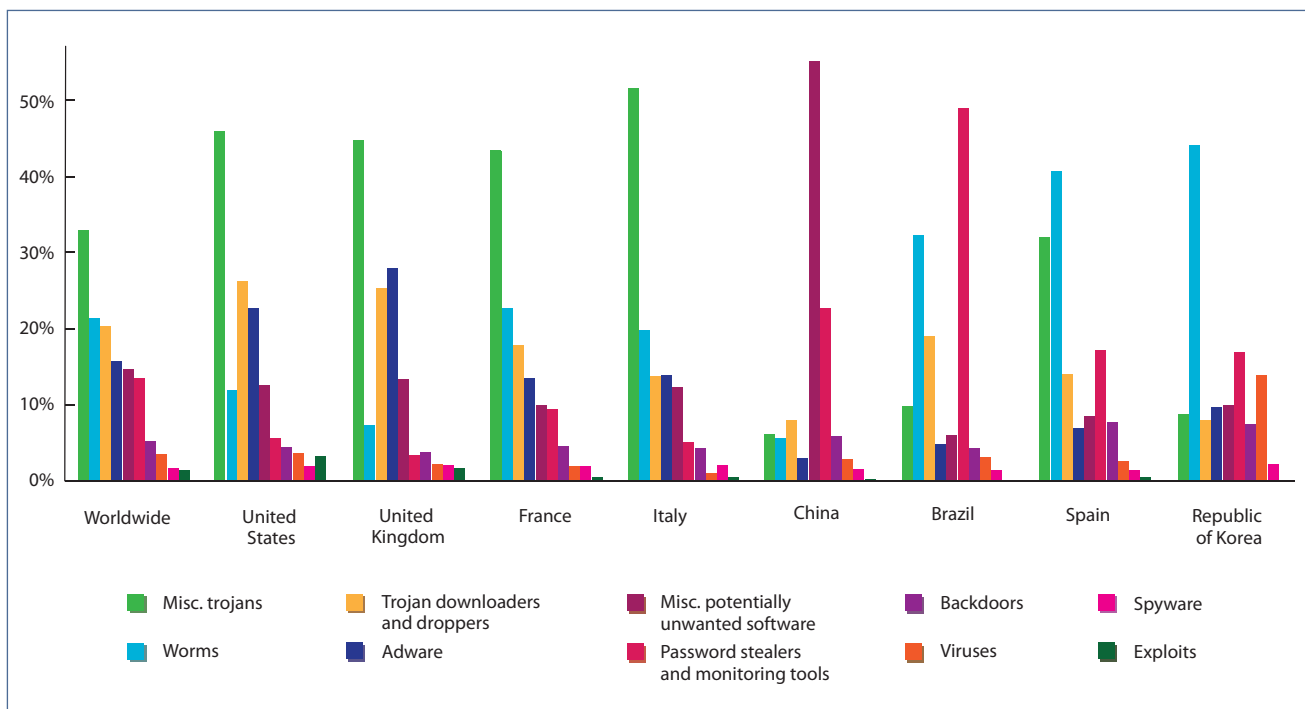
Country/Region	Computers cleaned 1H09	Computers cleaned 2H08	Change
UNITED STATES	13,971,056	13,245,712	5.5% ▲
CHINA	2,799,456	3,558,033	-21.3% ▼
BRAZIL	2,156,259	1,654,298	30.3% ▲
UNITED KINGDOM	2,043,431	2,225,016	-8.2% ▼
SPAIN	1,853,234	1,544,623	20.0% ▲
FRANCE	1,703,225	1,815,639	-6.2% ▼
REP. OF KOREA	1,619,135	1,368,857	18.3% ▲
ITALY	1,192,867	978,870	21.9% ▲
TURKEY	1,161,133	768,939	51.0% ▲
GERMANY	1,086,473	1,209,461	-10.2% ▼
MEXICO	957,697	915,605	4.6% ▲
CANADA	942,826	916,263	2.9% ▲
TAIWAN PROVINCE	781,214	466,929	67.3% ▲
RUSSIAN FEDERATION	581,601	604,598	-3.8% ▼
JAPAN	553,417	417,269	32.6% ▲

<sup>12</sup> *Microsoft Security Intelligence Report*, vol. 7, January through June 2009, <http://www.microsoft.com/sir> (last visited 8 January 2010).

Country/Region	Computers cleaned 1H09	Computers cleaned 2H08	Change
POLAND	551,419	409,532	34.6% ▲
NETHERLANDS	494,997	641,053	-22.8% ▼
AUSTRALIA	416,435	464,707	-10.4% ▼
PORTUGAL	375,502	337,313	11.3% ▲
BELGIUM	208,627	267,401	-22.0% ▼
SAUDI ARABIA	205,157	154,697	32.6% ▲
SWEDEN	197,242	287,528	-31.4% ▼
COLOMBIA	183,994	164,986	11.5% ▲
GREECE	161,639	158,476	2.0% ▲
DENMARK	160,001	224,021	-28.6% ▼

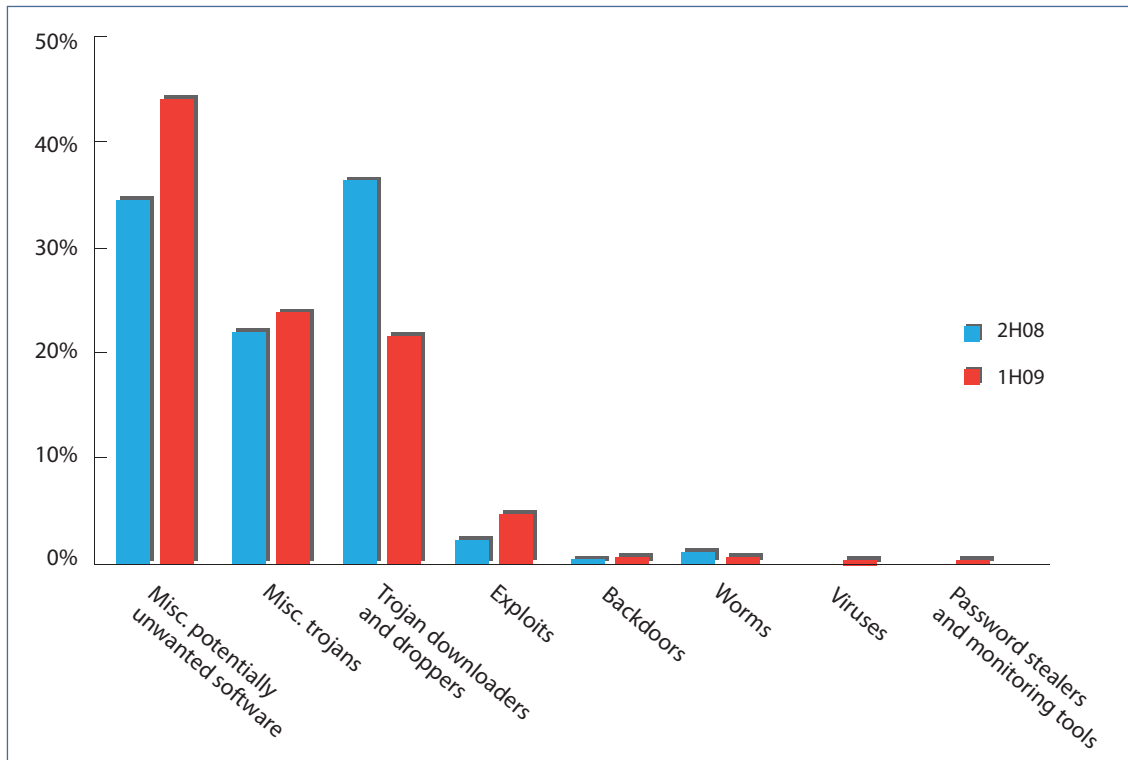
In the United States, the United Kingdom, France and Italy, trojans were the largest single category of threat; in China, several language-specific browser-based threats were prevalent; in Brazil, malware targeting online banking was widespread; in Spain and the Republic of Korea, worms dominated, led by threats targeting online gamers.

Figure 5. Threat categories worldwide and in the eight locations with the most computers cleaned by incidence among all computers cleaned 1H09



The Microsoft SmartScreen filter, introduced in Internet Explorer 8, provides phishing and anti-malware protection. Figure 6 details patterns of malware distribution detected by the SmartScreen Filter in 1H09.

Figure 6. Threats hosted at URL's blocked by the SmartScreen Filter, by category



Computers in enterprise environments (those running Microsoft Forefront Client Security)<sup>13</sup> were much more likely to encounter worms during 1H09 than home computers running Windows Live OneCare. Whereas the top threat detected in enterprise environments was the Conficker worm, Conficker was not in the top ten threats detected in home environments (see figure 7, opposite).

- More malware distribution sites are discovered on a daily basis than phishing sites.
- Malware hosting tends to be more stable and less geographically diverse.
- Miscellaneous trojans (including rogue security software) remained the most prevalent category.
- Worms rose from fifth place in 2H08 to become the second most prevalent category in 1H09.
- The prevalence of password stealers and monitoring tools also rose, due in part to increases in malware targeting online gamers.

Phishing impressions rose significantly in 1H09, due primarily to a large increase in phishing attacks targeting social networking sites (see figure 8, opposite).

Phishers continued to target a wider range of website types than in the past, with gaming sites, portals and the online presences of major corporations being some of the most frequently-targeted sites in 1H09.

<sup>13</sup> <http://www.microsoft.com/forefront/clientsecurity/en/us/default.aspx> (last visited 9 January 2010).



Figure 7. Threat categories removed by Windows Live OneCare and Forefront Client Security in 1H09 by percentage of all infected computers cleaned by each programme

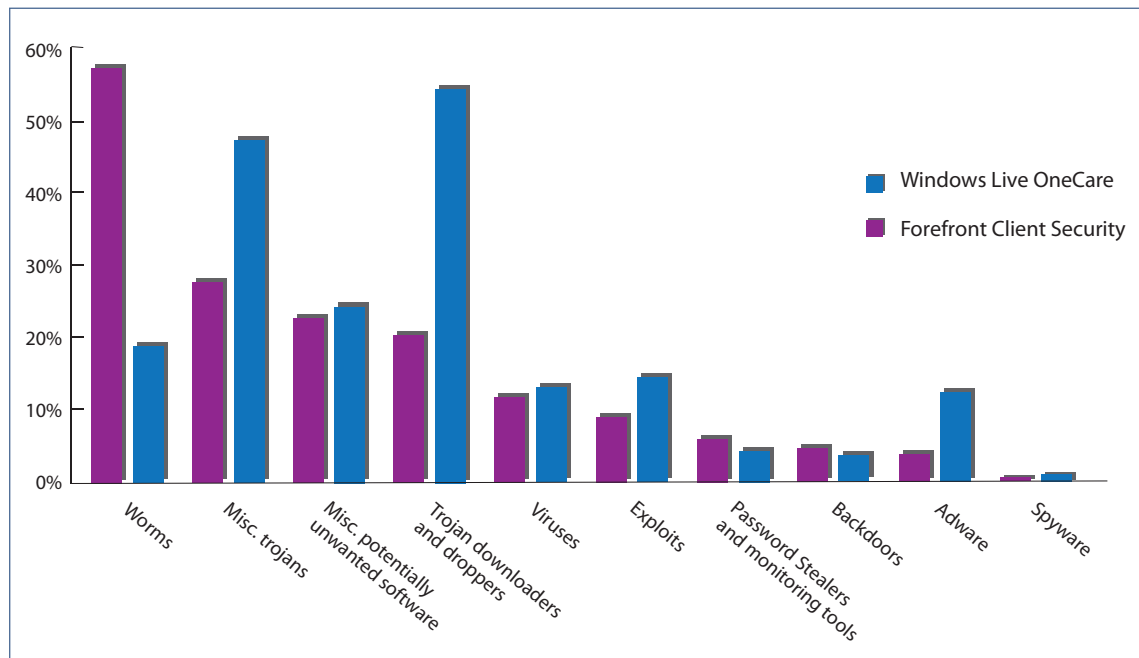
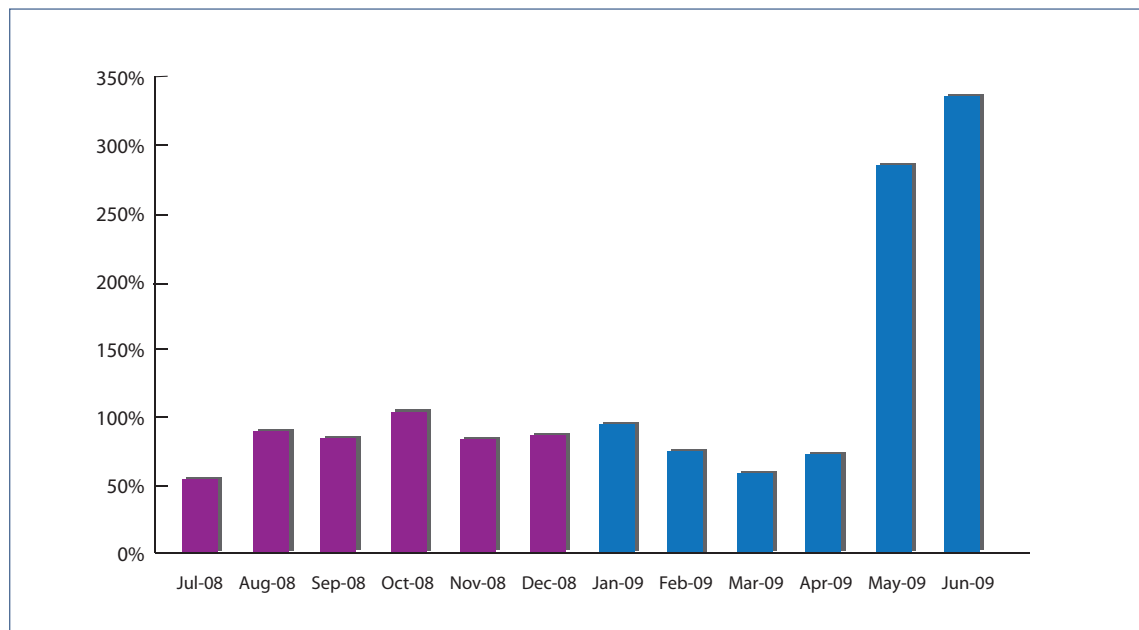
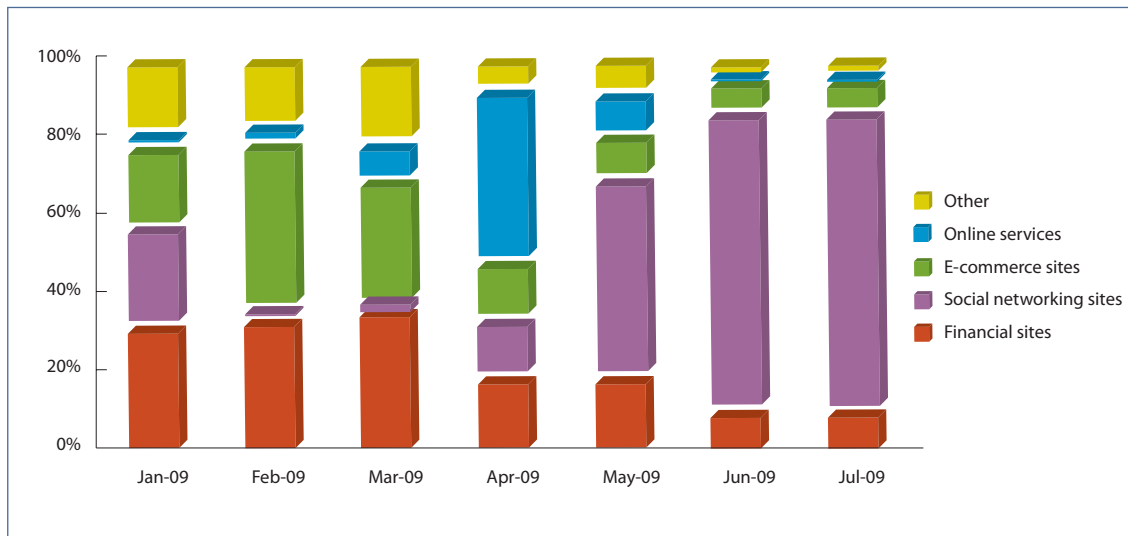


Figure 8. Phishing impressions tracked each month in 2H08 and 1H09, indexed to January 2009



After remaining mostly consistent throughout 2H08 and through April of 2009, the number of phishing impressions suddenly nearly quadrupled in May, and rose even higher in June due in part to a campaign or campaigns targeting social networks.

Figure 9. Impressions for each type of phishing site each month in 1H09



Financial institutions, social networks and e-commerce sites remain favoured targets for phishing attempts. Researchers also observed some diversification into other types of institutions, such as online gaming sites, webportals, and large software and telecommunications companies. Phishing sites are hosted all over the world on free hosting sites, on compromised webservers and in numerous other contexts. Performing geographic lookups on the IP addresses of the sites makes it possible to create maps showing the geographic distribution of sites and to analyse patterns.



## II. SCOPE OF THIS STUDY

### 1. Purpose

Elaboration of an inventory of best practices on public-private partnerships to prevent economic fraud and identity-related crime.

### 2. Background of the study

Starting with the release of a study on “Fraud and the Criminal Misuse and Falsification of Identity” in 2007, and on the basis of its mandates arising from ECOSOC resolutions 2004/26 and 2007/20, UNODC has launched a consultative platform on identity-related crime with the aim to bring together senior public sector representatives, business leaders, international and regional organizations and other stakeholders to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime.

In this context, a core group of experts was established to exchange views on the best course of action and the most appropriate initiatives that need to be pursued under the platform. The group has so far met three times in Courmayeur, Italy, on 29–30 November 2007, and in Vienna, Austria, on 2–3 June 2008 and 20–22 January 2009.

At all meetings, it was acknowledged that the cooperation between the public and private sector was essential in order to develop an accurate and complete picture of the problems posed by economic fraud and identity-related crime, as well as to adopt and implement both preventive and reactive measures against them.

On the recommendation of the Commission on Crime Prevention and Criminal Justice at its eighteenth session, the Economic and Social Council adopted Resolution 2009/22 of 30 July 2009, in which the Council requested UNODC, in consultation with Member States and taking into account relevant intergovernmental organizations and, in accordance with the rules and procedures of the Economic and Social Council, experts from academic institutions, relevant non-governmental organizations and the private sector, to collect, develop and disseminate, among others, “a set of material and best practices on public-private partnerships to prevent economic fraud and identity-related crime”.

In line with these guidelines and directions, the Corruption and Economic Crime Section of UNODC launched concrete follow-up work to build upon the recommendations of the

core group of experts and fulfil the mandate contained in ECOSOC resolution 2009/22 and, in this context, seeks the contribution of a consultant for the elaboration of an inventory of best practices on public-private partnerships to prevent economic fraud and identity-related crime.

### 3. Purpose of the study and specific issues to be covered

The purpose of the study is the accumulation and assessment of relevant research material and data and, based on that, the development of an inventory of best practices on public-private partnerships to prevent economic fraud and identity-related crime.

In gathering research material and drafting the inventory, the consultant should take into account the following:

- The report of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity (E/CN.15/2007/8 and Add. 1-3);
- The report of the first meeting of the core group of experts on identity-related crime (Courmayeur, Italy, 29–30 November 2007);
- The report of the second meeting of the core group of experts on identity-related crime (Vienna, Austria, 2–3 June 2008);
- The report of the third meeting of the core group of experts on identity-related crime (Vienna, Austria, 20–22 January 2009);
- The ongoing work in the G8 Lyon Group on related issues, where appropriate;
- The work of the Council of Europe on Internet-related theft, where appropriate;
- The work of the Organization for Economic Cooperation and Development (OECD) on online identity theft, where appropriate; and
- Other pertinent material, as appropriate.

The draft text of the inventory will be prepared by the consultant under the guidance and supervision of the Corruption and Economic Crime Section (CECS), UNODC.

The final text of the inventory will be used as working document for the fourth meeting of the core group of experts on identity-related crime, due to take place in Vienna, Austria, in January 2010.

The outcome of the study will also be submitted (as Conference Room Paper) to the Commission on Crime Prevention and Criminal Justice for its information at its nineteenth session, to be held in Vienna on 17–21 May 2010.

# III. PUBLIC-PRIVATE PARTNERSHIPS

## 1. Introduction

Cybercrime, irrespective of the different perspectives and interests involved, represents a common enemy which will only be defeated through partnership and cooperation. This new partnership approach will involve new structures and active participation by all parties, but with the Internet industry having a key role.

The accelerated development of the Internet over the last few years is one of the most significant societal phenomena of the century and resonates through the commercial, economic, cultural, social and moral aspects of our lives. Any evaluation of this significance must, however, take into account the fact that as a phenomenon, it is in a state of constant and rapid evolution and our traditional tools of measurement and analysis do not readily lend themselves to forecasting its effects or planning our future responses.<sup>14</sup>

Issues on the Internet are wide-ranging, technically and legally complex, and are international in their dimensions. They pose special challenges to the international community, governments, industry, educators, parents and, indeed, individual users of the Internet. New partnerships, new approaches and new levels of flexibility are needed to ensure that exploitation of the Internet incorporates safety measures specifically designed to ensure maximum protection for those who are vulnerable to its downside.

Because of the essential nature of the Internet, there are serious limits to what any one country can achieve on its own in the area of addressing cybercrime issues. The Internet itself is an international phenomenon in every sense of the word and any effective response hinges on high levels of international cooperation.

The responses to the challenges posed by cybercrime must be sufficiently flexible to reflect rapid changes in Internet technology and services. Measures which do not provide for review and adaptation are not suited to an environment characterized by this constant evolution.

The Internet operates on an international basis. The law operates on a territorial basis. Thus we have the genesis of many of the legal issues surrounding the Internet. Material on the Internet is held worldwide and can be accessed worldwide. Some material is held and accessed locally. Other material is held outside the jurisdiction and is only accessed locally.

<sup>14</sup> July 1998, "Illegal and Harmful Use of the Internet", first report of the working group, Irish Department of Justice, Equality and Law Reform, available at: [http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport\\_ie.pdf](http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport_ie.pdf) (last visited 10 January 2010).

The extent to which national law operates can therefore be a complex issue to decide. Liability issues often turn on the extent to which any particular party controls, or is aware of, illegal content. Common challenging features of cybercrime include cross-border search and seizure, mutual legal assistance, ease of mobility, speed of transactions, multi-lingual, multi-cultural and different legal jurisdictions.

Mr Nicola Dileone, High Technology Crime Centre, Europol, describes the challenge of international cybercrime and highlights the need for strong international cooperation when he describes that “a bad guy from China with an English name can target the French market selling Japanese equipment that can be paid using a Russian payment service by a Latvian middleman while using Swedish credentials for the registration of his domain with a Brazilian company, hosting the page in Thailand and refer to it from Iceland while communicating through an Indonesian mail server.”<sup>15</sup>

## 2. The benefits of public-private partnerships

Public-private partnerships are the primary approach to dealing with complex Internet problems today. Such a partnership is a strategic alliance or relationship between two or more strategic organizations. Successful partnerships are based on trust, equality and mutual understanding and obligations. Partnerships can be formal, where each party's roles and obligations are clearly outlined in a written agreement, or informal, where the roles and obligations are assumed or agreed to verbally.

A range of public-private partnerships exist today responding to cybercrime which cover the full spectrum of activities. There are partnerships between individual corporations who share information in areas of shared concern (such as FI-ISAC, which brings together financial institutions) or with a broader range of stakeholders (such as the London Action Plan which brings together law enforcement, industry, non-governmental organizations, etc). The level of participation, the reason for participation and the level of trust and sharing in that participation, all define the level of success of such public-private partnerships.

The EC Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime<sup>16</sup> state that a key objective is “strengthening the partnership between public authorities and the private sector so as to jointly design methods for detecting and preventing damage caused by criminal activities and for victimized companies to transmit relevant information concerning the frequency of offences suffered to the law enforcement agencies. In particular, it is recommended that the Commission work on the details of the guidelines adopted by the Conference on Global Cooperation Against Cybercrime, which met under the auspices of the Council of Europe on 1–2 April 2008, and which aimed at improving the partnership between public authorities and the private sector in the fight against cybercrime. In this context, the Council notes the recommendations made after the meeting of experts organized by the Commission on 25–26 September this year, attached in appendix”.

<sup>15</sup> Mr Nicole Dileone, “European Alert Platform”, High Technology Crime Centre, Europol, at the Public-Private Dialogue to Fight Online Illegal Activities hosted by the European Commission in Brussels, 27 November 2009.

<sup>16</sup> <http://register.consilium.europa.eu/pdf/en/08/st15/st15569.en08.pdf> (last visited 10 January 2010).

The first recommendation from these council conclusions expressed in the annex to the annex is: “law enforcement authorities and the private sector should be encouraged to engage in operational and strategic information exchange to strengthen their capacity to identify and combat emerging types of cybercrime. Law enforcement authorities should be encouraged to inform service providers about cybercrime trends.”

### 3. Raising awareness for fundamental principles of cooperation

An essential requirement for cooperation is respecting the fundamental principles of the parties involved:

- Service providers constantly balance the responsibility to protect customer information and comply with established privacy principles alongside cooperation efforts with law enforcement agencies to protect and promote public safety.

In this context, service providers typically establish criminal compliance programmes to help maintain that balance by evaluating demands and requests from law enforcement consistent with its legal obligations in applicable jurisdictions.

- Law enforcement agencies are mandated to investigate crime at a national level. Cybercrime, by its international dimension and constantly changing nature, requires substantial cooperation between national law enforcement agencies in different countries and access to knowledge, expertise and log records in the process of the crime investigation. The level of such knowledge and expertise varies within agencies and between agencies in different countries. The range of criminal procedural law is also very different.

### 4. Overcoming national and regional differences

Criminal compliance programmes vary greatly from one provider to the next depending on a number of factors, including, without limitation, the types of services offered and the location where customer records are stored. In some countries, therefore, certain providers will not offer any criminal compliance support, while in other regions the same providers may have elaborate compliance programmes in place.

### 5. Developing the foundation for a cooperation

An effective fight against cybercrime therefore requires a carefully considered approach from key stakeholders. With the complexity and speed of development of new technologies, such as new services being offered online for free, service providers are increasingly being asked to engage in a more active way, in addition to responding to requests from law enforcement. Law enforcement agencies do not have the capacity to develop internally all

the expertise that is required and cooperation with the private sector is not necessarily something done routinely. Law enforcement can gain and maintain an understanding of new technology areas from Internet service providers. Industry and law enforcement agencies need to share their expertise and concern.

At the very least, such cooperation takes place when law enforcement agencies request information from service providers. With experience, service providers can learn to understand which agencies are entitled to request information, and in what form. In return, law enforcement will learn what is the best time or best way to obtain the information they are looking for. At best, service providers who are filing complaints against fraudsters or abusers in order to protect their business services will understand the need to go beyond the raw criminal complaint and, in an appropriately sensitive way, provide, on a legal basis, further intelligence that will help law enforcement agencies better investigate the specific case reported by the service provider. This also helps law enforcement agencies better investigate cybercrime generally.

Regarding cooperation against cybercrime, there is a need for providing a framework that will ease this cooperation and make its value better understood for both sides, as well as for the general public.

On 16 May 2000, Jacques Chirac, President of the French Republic, at the G8 Conference on Security and Confidence in Cyberspace at the Elysee Palace, stated that “States cannot ensure security on the Internet without working with (businesses and associations) to establish the basis for genuine national and international co-regulation.” He went on to say that, “a dialogue between governments and the private sector is clearly essential. The G8 are convinced that faster or novel solutions should be developed and that government and industry must work together to achieve them.”<sup>17</sup>

## 6. Key indicators for successful public-private partnerships

- Participation of all key stakeholders;
- Equality of participation;
- Trust, transparency;
- Recognition of mutual strengths and weaknesses;
- Recognition that primary aims and responsibilities of each stakeholder vary;
- Focus on shared issues of concern rather than issues in conflict;
- Recognition that not all problems will be solved in such a partnerships;
- Sharing of knowledge, intelligence and experience in an atmosphere of mutual respect.

<sup>17</sup> Press release on the occasion of the G8 Conference on Security and Confidence in Cyberspace, Paris, Wednesday 17 May 2000, available at: <http://www.g7.utoronto.ca/crime/paris2000.htm> (last visited 10 January 2010).

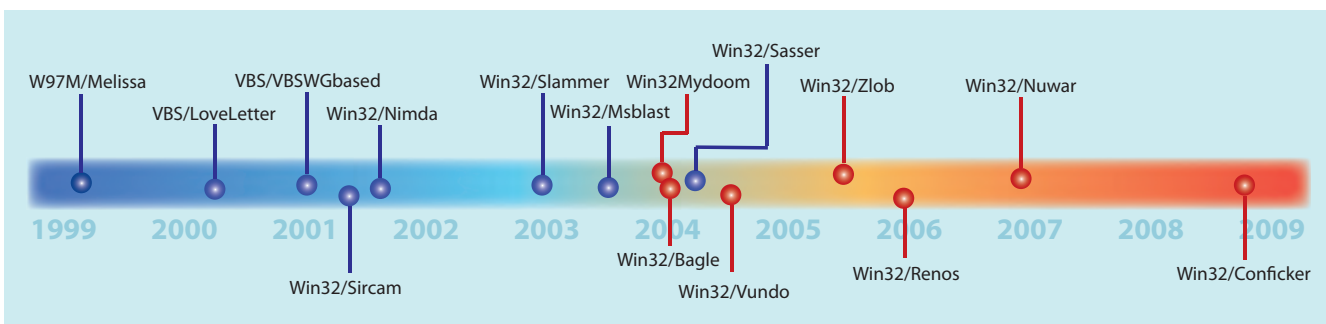


# IV. PREVENTING IDENTITY THEFT

## 1. Introduction

Preventing theft of personal information is not an expensive process, but requires a change in personal habits to include data privacy into daily behaviour. It rarely requires spending money on security products or even significant effort.

Figure 10. Malware timeline



Javelin Strategy and Research<sup>18</sup> identify six key guidelines to combat fraud. These are:

- Be vigilant—monitor your financial accounts regularly.
- Keep personal data private—think before you share personal information, including on social networking websites.
- Online is *safer* than *offline* when consumers use available security controls.
- Be aware of your surroundings and those around you.
- Ensure credit and debit cards are protected with zero liability from your financial institution.
- Learn about identity protection services.

These simple steps can provide sufficient protection for most types of identity theft crimes. Of course, they do not protect from attacks against databases or lost/stolen laptops which store personal information.

<sup>18</sup> Javelin Strategy and Research, 2009 Identity Fraud Survey Report: Consumer Version, *Prevent—Detect—Resolve*. February 2009, page 9. <http://www.javelinstrategy.com/products/CEDDA7/127/delivery.pdf> (last visited 9 January 2010).

For example, the most frequently-exploited vulnerabilities in Microsoft Office software during 1H09 were also some of the oldest.<sup>19</sup> More than half of the vulnerabilities exploited were first identified and addressed by Microsoft security updates in 2006. 71.2 per cent of the attacks exploited a single vulnerability for which a security update (MS06-027) had been available for three years. Computers which had this update applied were protected from all these attacks. The majority of Office attacks observed in 1H09 (55.5 per cent) affected Office programme installations that had last been updated between July 2003 and June 2004. Most of these attacks affected Office 2003 users who had not applied a single service pack or other security update since the original release of Office 2003 in October 2003.

It is suspected that many of these updates were not applied because the software was pirated in the first place, and this would be detected and rejected during the update process. Of course, if users were using properly licensed software *and* applied the current security updates, few of these attacks would have succeeded.

The increasing number of attacks, and the success of them, demonstrates the potential of this scam.<sup>20</sup> The number of unique phishing websites detected in June 2009<sup>21</sup> rose to 49,084, the highest recorded since April 2007's record number of 55,643 was reported to the APWG.<sup>22</sup> It is important to highlight that the scam is not limited to getting access to passwords for online banking. Offenders are aiming for access codes to computers and auction platforms as well as Social Security numbers.

## 2. Awareness raising

The majority of drive-by download pages<sup>23</sup> are hosted on compromised legitimate websites. Attackers gain access to legitimate sites through intrusion, or by posting malicious code to a poorly secured webform, like a comment field on a blog. Compromised servers acting as exploit servers can have massive reach; one exploit server can be responsible for hundreds of thousands of infected webpages. Exploit servers in 2009 were able to infect many thousands of pages in a short period of time.

There are a wide range of strategies to raise public awareness and consciousness about the issue of identity theft and providing support and advice to victims of identity theft. With credit card fraud, public awareness campaigns and stricter security controls encourage credit card owners to ensure that the card is never out of their sight.

<sup>19</sup> *Microsoft Security Intelligence Report*, vol. 7, January–June 2009, <http://www.microsoft.com/sir> (last visited 8 January 2010).

<sup>20</sup> In some phishing attacks up to 5 per cent of the victims provided sensitive information on the fake website. See *Dhamija/Tygar/Hearst, Why Phishing Works*, available at: [http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf), page 1, that are referring to *Loftness, Responding to "Phishing" Attacks*, Glenbrook Partners (2004).

<sup>21</sup> *Phishing Activity Trends Report for the first half of 2009*, available at: [http://www.antiphishing.org/reports/apwg\\_report\\_h1\\_2009.pdf](http://www.antiphishing.org/reports/apwg_report_h1_2009.pdf).

<sup>22</sup> Anti-Phishing Working Group. For more details, see: <http://www.antiphishing.org>.

<sup>23</sup> A programme that is automatically installed in your computer by merely visiting a website, without having to explicitly click on a link on the page. Typically spyware that reports information back to the vendor, drive-by downloads are deployed by exploiting flaws in the browser and operating system code. <http://www.yourdictionary.com/computer/drive-by-download> (last visited 9 January 2010).

Examples of online resources include:

- *Non-governmental organizations*  
PRC Privacy Rights Clearinghouse (PRC)  
<http://www.privacyrights.org/identity-theft-data-breaches>
- *Private persons*  
Robert Hartle  
<http://www.idtheft.org/>
- *Government*  
United States Department of Justice  
<http://www.justice.gov/criminal/fraud/websites/idtheft.html>
- *Commercial*  
SpendonLife.com: <http://wwwwww.spendonlife.com>  
Microsoft: <http://www.microsoft.com/protect/>

### 3. Security reports

Security reports provide essential intelligence to consumers and organizations about the spread of malware, phishing and other software vulnerabilities in order to empower users to combat the spread of these vulnerabilities through computers under their responsibilities. These reports are often researched and distributed at no cost, or more detailed versions are available for a commercial fee.

Examples of such reports include:

- *AntiPhishing Working Group Phishing Activity Trends Report*  
The APWG Phishing Activity Trends Report analyses phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website and by e-mail submissions. APWG also measures the evolution, proliferation and propagation of crimeware, drawing from the research of member companies. In the last half of the report are tabulations of crimeware statistics and related analyses.  
*Frequency:* Every 6 months  
*Cost:* Free
- *Javelin Strategy and Research Identity Fraud Survey Report*  
The Javelin 2009 Identity Fraud Survey Report: Consumer Version provides guidelines for consumers to help prevent, detect and resolve identity fraud. Over the past five years, Javelin has surveyed nearly 25,000 adults to find out the actual ways consumers are being affected by identity fraud in the United States. The results of the study are used to help educate consumers in order to lower their risk of identity fraud. The 2009 phone survey of almost 4,800 adults is the largest, most up-to-date study of identity fraud in the United States.  
*Frequency:* Annual  
*Cost:* Consumer version free, full version cost on website.

- *Microsoft Security Intelligence reports*

Microsoft® Security Intelligence Report provides an in-depth perspective on malicious and potentially unwanted software, software exploits, security breaches and software vulnerabilities (both in Microsoft software and in third-party software). Microsoft security products gather, with user consent, data from hundreds of millions of computers worldwide and from some of the Internet's busiest online services. Analysis of this data gives a comprehensive and unique perspective on malware and potentially unwanted software activity around the world. The Security Intelligence Report also offers strategies, mitigations and countermeasures.

*Frequency:* Every 6 months

*Cost:* Free

- *Symantec Global Internet Security Threat Report<sup>24</sup>*
- *Symantec EMEA Internet Security Threat Report<sup>25</sup>*
- *Symantec Government Internet Security Threat Report<sup>26</sup>*

The Symantec Global/EMEA/Government Internet Security Threat Reports provide an annual overview and analysis of Internet threat activity, a review of known vulnerabilities, and highlights of malicious code. Trends in phishing and spam are also assessed, as are observed activities on underground economy servers. Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. More than 240,000 sensors in over 200 countries monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

*Frequency:* Every 6 months

*Cost:* Free

- *Websense Security Labs State of Internet Security<sup>27</sup>*

Websense® Security Labs™ uses the patent-pending Websense ThreatSeeker™ Network to discover, classify and monitor global Internet threats and trends. Featuring the world's first Internet HoneyGrid™, the system uses hundreds of technologies including honeyclients, honeypots, reputation systems, machine learning and advanced grid computing systems to parse through more than one billion pieces of content daily, searching for security threats.

*Frequency:* Every 6 months

*Cost:* Free

<sup>24</sup>[http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_internet\\_security\\_threat\\_report\\_xiv\\_04-2009.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf) (last visited 9 January 2010).

<sup>25</sup> [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_emea\\_internet\\_security\\_threat\\_report\\_04-2009.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_emea_internet_security_threat_report_04-2009.en-us.pdf) (last visited 9 January 2010).

<sup>26</sup> [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_government\\_internet\\_security\\_threat\\_report\\_04-2009.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_government_internet_security_threat_report_04-2009.en-us.pdf) (last visited 9 January 2010).

<sup>27</sup> [http://www.websense.com/site/docs/whitepapers/en/WSL\\_Q1\\_Q2\\_2009\\_FNL.PDF](http://www.websense.com/site/docs/whitepapers/en/WSL_Q1_Q2_2009_FNL.PDF) (last visited 9 January 2010).

## 4. End-user training

ICT services produce vast quantities of personal data:<sup>28</sup>

- 65 billion phone calls per year;
- 2 million e-mails per second;
- 1 million instant messenger messages per second;
- 8 terabytes traffic per second;
- 255 exabytes magnetic storage;
- 1 million voice queries per hour;
- 2 billion location nodes activated;
- 600 billion RFID tags in use.

Most end-user training is based on mass media warnings (public service announcements on television or radio), leaflets distributed by retail banking outlets or by Internet service providers. Some online services are available which offer web-seminars (webinars) or online videos on You-Tube, etc.

## 5. Policy development

*Council of Europe*

### Cybercrime Convention

The Convention on Cybercrime, entered into force on 1 July 2004, is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures, such as the search of computer networks and interception.

Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

*Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime*

These Guidelines for the cooperation between law enforcement agencies and Internet service providers against cybercrime<sup>29</sup> were adopted at the Octopus Conference on 1–2 April 2008.

<sup>28</sup> *Kevin Kelly*, December 2007, [http://www.ted.com/index.php/talks/kevin\\_kelly\\_on\\_the\\_next\\_5\\_000\\_days\\_of\\_the\\_web.html](http://www.ted.com/index.php/talks/kevin_kelly_on_the_next_5_000_days_of_the_web.html) (last visited 10 January 2010).

<sup>29</sup> [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567\\_prov-d-guidelines\\_provisional2\\_3April2008\\_en.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf) (also available in French, Romanian, Russian, Spanish and Ukrainian) (last visited 10 January 2010).

They recognize that building an information society requires the strengthening of trust in information and communications technologies (ICT's), the protection of personal data and privacy and the promotion of a global culture of cyber-security in a context where societies worldwide are increasingly dependent on ICT and thus vulnerable to cybercrime.

The Guidelines are not intending to substitute existing legal instrument, but assume adequate legal instruments exist that provide a well-balanced system of investigation instruments as well as related safeguards and a protection of fundamental human rights, such as freedom of expression, the respect for private life, home and correspondence and the right to data protection. It is therefore recommended that States adopt regulations in their national law in order to fully implement the procedural provisions of the Convention on Cybercrime and to define investigative authorities and obligations of law enforcement, while putting in place conditions and safeguards as foreseen in Article 15 of the Convention. This will:

- Ensure efficient work of law enforcement authorities;
- Protect the ability of Internet service providers to provide services;
- Ensure that national regulations are in line with global standards;
- Promote global standards instead of isolated national solutions; and
- Help ensure due process and the rule of law, including principles of legality, proportionality and necessity.

In order to enhance cyber-security, minimize use of services for illegal purposes and build trust in ICT, it is essential that Internet service providers and law enforcement authorities cooperate with each other in an efficient manner with due consideration to their respective roles, the cost of such cooperation and the rights of citizens.

The purpose of the present Guidelines is to help law enforcement authorities and Internet service providers structure their interactions in relation to cybercrime issues. They are based on existing good practices and should be applicable in any country around the world in accordance with national legislation and respect for the freedom of expression, privacy, the protection of personal data and other fundamental rights of citizens.

The European Court of Human Rights referred to the Guidelines for the first time in the case of *K.U v. Finland*<sup>30</sup>. The Guidelines are presented as relevant international materials applying in this case related to the protection of the right to respect for private and family life (Article 8 of the European Convention for Human Rights).

### *European Commission*

The EC Council conclusions of 27 November 2008 invited Member States and the Commission, in particular, to draft, in consultation with private operators, a European agreement model for cooperation between law enforcement agencies and private operators.

<sup>30</sup> [http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/LEA\\_ISP/1429\\_ECHR\\_CASE\\_OF\\_K.U.\\_v%20Finland.pdf](http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/1429_ECHR_CASE_OF_K.U._v%20Finland.pdf) (last visited 10 January 2010).

The framework decisions listed below made punishable respectively: the dissemination of child pornography; incitement to racist and xenophobic violence or hatred; provocation to commit terrorist attacks, terrorist recruitment and training legislation, also when it takes place online:

The Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (OJ L 13 of 20 January 2004, page 44),

The Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (OJ L 328 of 6 December 2008, page 55) and,

The Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (OJ L 330 of 9 December 2008, page 21).

Main issues covered:

- Different kinds of illegal content—same solutions?
- Freedom of speech and cases where the illegality is difficult to assess.
- Different national realities—same solutions?
- Codes of conduct on notice and take down.
- General Conditions of Contracts to prevent the liability of private operators.
- Elements of a European agreement model.
- Format of the dialogue LEAs–ISPs.
- Objectives of the dialogue LEAs–ISPs: raising awareness and promoting cooperation.

## *UNODC*

On the recommendation of the Commission on Crime Prevention and Criminal Justice at its thirteenth session in 2004, the Economic and Social Council adopted resolution 2004/26 on “International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes”. In that resolution, the Council encouraged, inter alia, “Member States to cooperate with one another in efforts to prevent and combat fraud and the criminal misuse and falsification of identity, including through the United Nations Convention against Transnational Organized Crime<sup>31</sup> and other appropriate international instruments, and to consider the review of domestic laws on fraud and the criminal misuse and falsification of identity, where necessary and appropriate, to facilitate such cooperation”.

<sup>31</sup> General Assembly resolution 55/25, annex I.

On the recommendation of the Commission on Crime Prevention and Criminal Justice at its sixteenth session in 2007, the Economic and Social Council adopted resolution 2007/20 on “International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime”. In that resolution, the Council, *inter alia*, encouraged:

15. Member States to take appropriate measures so that their judicial and law enforcement authorities may cooperate more effectively in fighting fraud and identity-related crime, if necessary by enhancing mutual legal assistance and extradition mechanisms, taking into account the transnational nature of such crime and making full use of the relevant international legal instruments, including the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption;

16. Member States to consult and collaborate with appropriate commercial and other private sector entities to the extent feasible, with a view to more fully understanding the problems of economic fraud and identity-related crime and cooperating more effectively in the prevention, investigation and prosecution of such crime; and

17. The promotion of mutual understanding and cooperation between public and private sector entities through initiatives aimed at bringing together various stakeholders and facilitating the exchange of views and information among them, and requests the United Nations Office on Drugs and Crime, subject to extrabudgetary resources, to facilitate such cooperation, in consultation with the secretariat of the United Nations Commission on International Trade Law, pursuant to Economic and Social Council resolution 2004/26 of 21 July 2004.

Furthermore, on the recommendation of the Commission on Crime Prevention and Criminal Justice at its eighteenth session in 2009, the Economic and Social Council adopted resolution 2009/22 on “International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime”. In that resolution, the Council requested:

7. the United Nations Office on Drugs and Crime, in consultation with Member States and taking into account relevant intergovernmental organizations and, in accordance with the rules and procedures of the Economic and Social Council, experts from academic institutions, relevant non-governmental organizations and the private sector, to collect, develop and disseminate:

(a) Material and guidelines on the typology of identity-related crime and on relevant criminalization issues to assist Member States, upon request, in the establishment of new identity-based criminal offences and the modernization of existing offences, taking into account the pertinent work of other intergovernmental organizations engaged in related matters;

(b) Technical assistance material for training, such as manuals, compilations of useful practices or guidelines or scientific, forensic or other reference



material for law enforcement officials and prosecution authorities in order to enhance their expertise and capacity to prevent and combat economic fraud and identity-related crime;

(c) A set of useful practices and guidelines to assist Member States in establishing the impact of such crimes on victims;

(d) A set of material and best practices on public-private partnerships to prevent economic fraud and identity-related crime;

[...]

10. The United Nations Office on Drugs and Crime to continue its efforts, in consultation with the United Nations Commission on International Trade Law, to promote mutual understanding and the exchange of views between public and private sector entities on issues related to economic fraud and identity-related crime, with the aim of facilitating cooperation between various stakeholders from both sectors through the continuation of the work of the core group of experts on identity-related crime, the composition of which should respect the principle of equitable geographical distribution, and to report on the outcome of its work to the Commission on Crime Prevention and Criminal Justice on a regular basis.

#### *Recent seminars and events*

- On 23 October, the EDPS, together with the European Network and Information Security Agency (ENISA) hosted a seminar on “Responding to Data Breaches” in the European Parliament. The seminar was devoted to three main objectives, which correspond to the “life cycle of data breach”: sharing and exploring best practices for preventing and mitigating the occurrence of data breaches from a data controller point of view; exchanging best practices developed by data protection authorities, as well as institutional and industry stakeholders on how to manage security breaches, including the development of procedures aimed at investigating breaches; gathering experience on data breach notification management from other sectors and from non-EU member States.
- On 27 November 2009 in Brussels, the European Commission hosted a conference on “Public-Private Dialogue to Fight Online Illegal Activities”.
- On 23–24 November 2009 in Zagreb, Croatia, the OSCE hosted a National Expert Workshop on a Comprehensive Approach to Cyber Security Addressing Terrorist Use of the Internet, Cybercrime and Other Threats. Sessions covered Terrorist use of the Internet/Cyber attacks by terrorist groups—Countermeasures, Legal Frameworks, Best Practices and PPPs, Cybercrime—Countermeasures, Legal Frameworks, Best Practices and PPPs and Threats to Critical Infrastructures/Other threats—Countermeasures, Legal Frameworks, Best Practices and PPPs.
- On 9–10 November 2009 in Bern, Switzerland, the third European FI-ISAC Meeting was hosted with participation from the international banking sector, law

enforcement agencies, computer emergency response teams (CERTs) and National and EU level policy makers with the aim to create a trusted environment where stakeholders could freely share information about cybercrime in the financial sector and experience of national cooperations.

### *Financial institutions*

#### Information Sharing and Analysis Center Europe (FI-ISAC)

It is important for financial institutions to share information on vulnerabilities, incidents and measures and to know the modus operandi of attacks. Information security is not a competitive issue. Trust and value grow together but need investment in time and energy and information sharing is very successful in small groups with consistent membership since it is based on personal factors.

As it is very important to build trust, the FI-ISAC operate a strict information sharing protocol (TLP) called the traffic light model. Information, documents or sessions which are considered “red” cover on-going incidents and information from law enforcement and state secret services. These sessions are delivered verbally and are not recorded during meetings. “Yellow” covers information that is meant for further distribution within the bank or the (ICT) service provider. Such information is considered confidential but not top secret. It is anonymised and distributed via closed FI-ISAC list server. “Green” has no rules for disclosure.

The European FI-ISAC network is currently supported by ENISA and works very well at raising awareness about (information) security and especially at management level inside financial institutions. The regular meetings provide substantial added value for all participants. The long term sustainability of such an activity is a key concern.

#### Bederlandse Vereniging van Banken<sup>32</sup>

NVB has 90 member banks in the Netherlands and strives towards a strong, healthy and internationally competitive banking industry in the Netherlands. Representing the common interests of the banking sector, it strives towards the effective operation of market forces whilst taking into account the interests of its interlocutors.

In 2008, the Netherlands had:

- 1.7 billion POS transactions;
- 600 million ATM transactions;
- More than 50 per cent of domestic payments made via the Internet;

<sup>32</sup> *Michael Samson*, National Infrastructure against Cybercrime, A public-private partnership—Management of data breaches, Netherlands Bankers’ Association, Brussels, 23 October 2009, [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar\\_data\\_breaches\\_presentations\\_EN.zip](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar_data_breaches_presentations_EN.zip) (last visited 10 January 2010).

- 28 million iDEAL transactions;
- Skimming fraud of €31 million;
- No fraud statistics on e-banking.

*NICC (National Infrastructure (against) CyberCrime sponsored by Department of Economic Affairs)*. Embracing the principle of “learning by doing”, the Dutch government and the private sector took the first steps towards developing a successful strategy against cybercrime in 2006 with the establishment of the National Infrastructure against Cybercrime (Nationale Infrastructuur ter bestrijding van Cybercrime, NICC).<sup>33</sup> An infrastructure is needed to integrate separate activities and establish and facilitate collaboration between all the parties involved.

The NICC programme is charged with the responsibility of creating this infrastructure—not only by developing new features, but by collaborating with others as much as possible and by integrating existing initiatives in order to create the national infrastructure.

A number of Dutch organizations involved in the fight against cybercrime are already in place, such as the Cybercrime Reporting Unit (Meldpunt Cybercrime), the High Tech Crime Team of the National Police Services Agency (Korps Landelijke Politiediensten, KLPD) and the National Alerting Service (Waarschuwingsdienst.nl) of GOVCERT.NL, the government’s Computer Emergency Response Team.

The fight against cybercrime at the national level is currently still fragmented, however, as there is no comprehensive overview available of all the initiatives. It is not clear who is responsible for what, and there is no common, public-private, integrated approach. The map of the fight against cybercrime has overlapping features and “blind spots”. The NICC assesses the status of the fight against cybercrime, identifies overlaps and supports activities that help fill in these blind spots.

The Cybercrime Information Exchange is the beating heart of the Dutch National Infrastructure, in which public and private organizations share sensitive information.

### Irish Banking Federation (IBF)

The Irish Banking Federation (IBF)<sup>34</sup> is the leading representative body for the banking and financial services sector in Ireland. The membership comprises banks and financial services institutions, both domestic and international, operating in Ireland. It published a consumer Fraud Prevention Guide 2009 in conjunction with the Irish Payment Services Organisation, the Garda Síochána and the Police Service of Northern Ireland. It participates in a multi-sector Irish Banking Federation Hi-Tech Crime Forum, whose membership consists of all retail banks operating in Republic of Ireland, An Garda Síochána, Internet Service Providers Association and UCD CCI. Its mission is similar to FI-ISAC to share knowledge about techniques used by criminals which helps to build up reactive capability.

<sup>33</sup> [http://www.samentegencybercrime.nl/UserFiles/File/Leaflet\\_NICC.pdf](http://www.samentegencybercrime.nl/UserFiles/File/Leaflet_NICC.pdf) (last visited 10 January 2010).

<sup>34</sup> <http://www.ibf.ie/> (last visited 10 January 2010).

In 2008, Ireland had:

- 202.5 million ATM withdrawals;
- 2.3 million credit cards in use (2007);
- 181 million transactions on 2.9 million debit cards;
- 2.4 million customers registered for online banking by June 2009;
- Customers who accessed online account balances 67.1 million times by June 2009;
- Customers who made 16.9 million payments online.

## Industry

### EuroISPA—European ISP Association

EuroISPA is recognized as the voice of the European ISP industry and is the largest “umbrella” association of Internet service providers in the world representing more than 1,700 ISPs in Europe.

EuroISPA believe that public-private cooperation does already exist.<sup>35</sup> However, there is need for improvement by:

- Raising awareness;
- Enhancing culture of cooperation at national level between administrative and judicial authorities and industry;
- Enhancing LEA cooperation across Member States;
- International cooperation and dialogue beyond EU;
- Developing expertise: training of judges and prosecutors is a challenge both at national and international level;
- Balancing privacy rights v. LEA requests;
- Discussing reimbursement of costs of law enforcement requests;
- Overcoming legal challenges created by the variety of legal systems.

On 20 March 2006, EuroISPA hosted a roundtable panel in Brussels on “A Coordinated Approach to Online Fraud: Combating Phishing”, which was supported by Interpol and Microsoft. At the event EuroISPA President, Professor Michael Rotert, stated that “phishing is a threat to all online industry stakeholders’ efforts to increase the availability and take-up of online services. Hence, the partnerships that joint efforts between industry, policy-makers, law enforcement and consumers create and strengthen are really vital if our industry is to effectively counter this threat. We hope that this initiative will stimulate

<sup>35</sup> Cyber criminality: the private sector perspective, *Michael Rotert*, Vice-President, EuroISPA, joint presentation in conjunction with ETNO, the European Telecommunications Network Operators Association (which represents 43 companies from 36 countries) at the Public-Private Dialogue to Fight Online Illegal Activities hosted by the European Commission in Brussels, 27 November 2009.

further stakeholders to counter phishing”.<sup>36</sup> EuroISPA’s commitment to raising awareness about phishing follows the launch of its dedicated anti-phishing website in October 2005. This site, developed with the support of eBay, contains tips and concise information on anti-phishing and can be viewed at [www.euroispa.org/antiphishing](http://www.euroispa.org/antiphishing) [no longer available online from 10 June 2010 but available on [www.archive.com](http://www.archive.com)].

### The London Action Plan<sup>37</sup>

On 11 October 2004, government and public agencies from 27 countries responsible for enforcing laws concerning spam met in London to discuss international spam enforcement cooperation. At this meeting, a broad range of spam enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies, met to discuss international spam enforcement cooperation. Several private sector representatives also collaborated in parts of the meeting.

Global cooperation and public-private partnerships are essential to spam enforcement, as recognized in various international fora. Building on recent efforts in organizations such as the Organisation for Economic Cooperation and Development (OECD) and the OECD Spam Task Force, the International Telecommunications Union (ITU), the European Union (EU), the International Consumer Protection Enforcement Network (ICPEN) and the Asia-Pacific Economic Cooperation (APEC), the participants issued an action plan.

The purpose of this action plan is to promote international spam enforcement cooperation and address spam related problems, such as online fraud and deception, phishing and dissemination of viruses. The participants also opened the action plan for participation by other interested government and public agencies, and by appropriate private sector representatives, as a way to expand the network of entities engaged in spam enforcement cooperation.

### Sixth German Anti Spam Summit<sup>38</sup>

The sixth German Anti Spam Summit took place from 27–29 October in Wiesbaden, focusing on lottery spam and other advance fee frauds committed via e-mail. Organizers were eco, the Contact Network of Spam Authorities (CNSA), the London Action Plan (LAP), Hessen-IT and ENISA. It was sponsored by Microsoft, eleven, Cloudmark, Iron-Port and clara.net. The first day of the event was reserved exclusively for CNSA/LAP-members’ training.

During the following two days, experts from around the globe presented and discussed the latest legal and technical development in the area of Spam. Speakers represented law enforcement agencies, industry, awareness raising organizations and universities. Wednesday’s agenda focused in particular on advance-fee frauds.

<sup>36</sup> EuroISPA Press Release: 20 March 2006 “EuroISPA hosts multi-stakeholder event on combating phishing”.

<sup>37</sup> <http://www.londonactionplan.com/> (last visited 10 January 2010).

<sup>38</sup> <http://www.eco.de/veranstaltungen/6dask.htm> (last visited 10 January 2010).



# V. SUPPORTING INVESTIGATIONS INTO IDENTITY THEFT

In addition to standard criminal behaviour, which has now moved online, the Internet has seen a new range of crimes emerge. Ever since the first generation of computer- and network-related attacks took place, new scams have been discovered. These crimes, such as “phishing”<sup>39</sup> and “identity theft”,<sup>40</sup> require new methods of investigation and rely heavily on data and information in the hands of Internet industry to achieve a successful prosecution. A lack of cooperation can seriously hinder the investigation.

## 1. Detecting crime and collecting evidence

Identity theft is a crime that can go on for a long period of time without being detected. Identity theft itself is very difficult to detect and reports only come from organizations that lose data.

### *Data breaches*

There are many examples of this, including when thousands of customers of United Kingdom insurer Standard Life were put at risk of fraud after their personal details were lost by HM Revenue and Customs (HMRC). The data on 15,000 pension policy holders was sent on a CD from HMRC offices in Newcastle to Standard Life’s Edinburgh headquarters by courier, but never arrived.<sup>41</sup> The lost disk contained names, national insurance numbers, dates of birth, addresses and pension data. Information like this would easily lend itself to abuse by crooks if it fell into the wrong hands. Providing fraudsters were able to read the disk, they might be able to apply for loans or credit cards under false names.

<sup>39</sup> Regarding the phenomenon “phishing”, see *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: [http://people.seas.harvard.edu/~rachna/papers/why\\_phishing\\_works.pdf](http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf); Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: [http://www.usdoj.gov/opa/report\\_on\\_phishing.pdf](http://www.usdoj.gov/opa/report_on_phishing.pdf).

<sup>40</sup> Regarding the phenomenon “identity theft”, see, for example: *Gercke*, Internet-related Identity Theft, 2007, available at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/combating\\_economic\\_crime/3\\_Technical\\_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf](http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf); *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, *Lex Electronica*, vol. 11, No. 1, 2006, available at: [http://www.lex-electronica.org/articles/v11-1/chawki\\_abdel-wahab.pdf](http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf) (last visited November 2007); *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: [http://www.privacyrights.org/ar/id\\_theft.htm](http://www.privacyrights.org/ar/id_theft.htm) (last visited November 2007).

<sup>41</sup> [http://www.theregister.co.uk/2007/11/05/standard\\_life\\_lost\\_cd\\_security\\_flap/](http://www.theregister.co.uk/2007/11/05/standard_life_lost_cd_security_flap/) (last visited January 10, 2010).

Another example in the United Kingdom was in March 2007, when two CDs containing personal details of 25 million people were lost by HM Revenue and Customs, causing the resignation of HMRC chairman Paul Gray<sup>42</sup> and requiring Prime Minister Gordon Brown to stand up in Parliament and apologise for the loss.<sup>43</sup> He apologised in the Commons for the “inconvenience and worries” caused and said the government was working to prevent the data being used for fraud. There have been many other examples of similar incidents of data loss<sup>44</sup> over the years.

### *Data breach disclosure*

In 2003, California was the first state to adopt a data breach disclosure law (SB1386), and it has been the model by which most other North American states developed their laws. Disclosure laws require firms to notify individuals when their personal information has been lost or stolen. Although features of the laws differ greatly across states, the overall objectives are to inform consumers, incentivize investments in security and to reduce ID theft.<sup>45</sup> Many laws were titled “identity theft prevention”. Strangely, research conducted by Alessandro Acquisti and Sasha Romanosky from Carnegie Mellon University indicate that both data breaches and identity theft crimes are increasing, but also suggest that identity theft for North American states both with and without disclosure law appear to follow same trend.<sup>46</sup>

Due to the fear and panic caused by such data failures in Europe, the EC is now considering the adoption of mandatory reporting of data breaches.<sup>47</sup> With the EC telecoms reform, the EC will strengthen and clarify current data protection rules. When a security breach happens, the operator will have to inform the authorities and those citizens who are at risk as a result of the loss of their personal data. Furthermore, network operators must notify the competent national regulatory authority of a breach of security or loss of integrity that had a significant impact on the operation of networks or services. According to Ms Viviane Reding, “Transparency and information will be the key new principles for dealing with breaches of data security.”

Lieutenant-Colonel Eric Freyssinet DGGN/SDPJ from the French Gendarmerie highlights the reasons why data breach reporting is a problem for many companies.<sup>48</sup> These are that the legal process is often seen as adverse: due to publicity of the trial, investigations against companies which do not secure personal data appropriately and fear of the impact

<sup>42</sup> [http://news.bbc.co.uk/2/hi/uk\\_news/politics/7104368.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/7104368.stm) (last visited 10 January 2010).

<sup>43</sup> <http://news.bbc.co.uk/2/hi/7104945.stm> (last visited 10 January 2010).

<sup>44</sup> [http://news.bbc.co.uk/2/hi/uk\\_news/7103911.stm](http://news.bbc.co.uk/2/hi/uk_news/7103911.stm) (last visited 10 January 2010).

<sup>45</sup> *Alessandro Acquisti, Sasha Romanosky*, Carnegie Mellon University, “Responding to Data Breaches”, European Parliament, 23 October 2009 [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar\\_data\\_breaches\\_presentations\\_EN.zip](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar_data_breaches_presentations_EN.zip) (last visited 10 January 2010).

<sup>46</sup> *Idem*.

<sup>47</sup> “The Telecoms Reform has put the issue of mandatory notification of personal data breaches firmly on the European policy agenda. The reformed telecoms package, now awaiting final agreement, will establish rules concerning the prevention, management and reporting of data breaches in the electronic communications sector.” Speech by Ms Viviane Reding, Member of the European Commission responsible for Information Society and Media EDPS-ENISA Seminar “Responding to Data Breaches”, Brussels, 23 October 2009, [http://ec.europa.eu/commission\\_barroso/reding/docs/speeches/2009/brussels-20091023.pdf](http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/brussels-20091023.pdf) (last visited 10 January 2010).

<sup>48</sup> “Responding to data breaches”, European Parliament Brussels, October 23, 2009, [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar\\_data\\_breaches\\_presentations\\_EN.zip](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/Seminar_data_breaches_presentations_EN.zip) (last visited 10 January 2010).



of law enforcement activity on the system. He also notes that there is a need for balance between legal obligations and best practice, since there is a common interest to share information about breaches and, when necessary, to initiate criminal investigations.

### *Signal Spam*

However, there are also some PPP initiatives which are encouraging users to report crime. “Signal Spam” is an initiative created in France with a wide range of public and private stakeholders.

Spam is a multifaceted phenomenon, cause of multiple threats to the citizens and to the information society. This is why the French government implemented a national initiative in 2005 that would address this challenge in a comprehensive manner based on a partnership between public and private sectors entitled Signal Spam.

Signal Spam empowers citizens to report any kind of spam of which they are victim, and it provides authorities and interested companies real-time access to these reports to ensure Internet safety and enable enforcement. Signal Spam is unique in the fact it combines all interested parties, from legitimate e-mail marketing to security companies, Internet service providers and industry organizations, as well as administrative authorities and law enforcement agencies.

Thanks to the invaluable information provided directly by the users, Signal Spam allows public authorities to constantly assess the threats and take action against fraudulent or criminal activities committed on the network. Signal Spam allows companies to identify attacks conducted against their services and brands, and to improve the protection of its customers.

Spam is more than ever a problem for Internet users. In June 2009, various institutes estimated that between 180 and 200 billion spam messages are sent daily worldwide, representing over 90 per cent of e-mails.

Currently, a user in Europe receives, on average, a dozen spam messages a day to his or her professional and personal e-mail addresses. Spam, scam (that is to say, mail fraud) and phishing (attempts to identity theft, or access to online accounts) are all manifestations of the same problem. What is known under the generic term “spam” refers to several types of messages that can convey counterfeit scams and even viruses.

The French government, aware of the magnitude and complexity of the phenomenon, decided to act. The Third Inter-Ministerial Committee for the Information Society (CISI) in July 2003 tasked the Department of Media Development to implement a series of measures to fight spam.

The work led to the creation of the non-profit association Signal Spam in November 2005, and to the launch of a tool for reporting spam and the website [www.signalspam.fr](http://www.signalspam.fr) on 10 May 2007. Signal Spam is an association which includes most of the French organizations involved in the fight against spam, whether government or Internet professionals. It aims to unite all efforts to fight against the plague of spam.

A key prerequisite is that the reports received have a legal value and could be used in court, therefore the users reporting spam are identified by a registration process on the Signal Spam website. If they wish so, their reports can be used in judicial and administrative actions. The fact that a single database, fed directly by reports from citizens, can be accessed by both private and public entities, makes Signal Spam a unique initiative. In the two years since the launch of Signal Spam, 17 million alerts were received. The reports are mainly through plug-ins, which can be downloaded by the user and installed on Microsoft Outlook or Thunderbird.

Today, attacks are more targeted and their total number is on the increase. Massive and untargeted spam campaigns belong to the past, as technology filters have improved. For example, a phishing attack used to consist of tens or hundreds of thousands of e-mails. Now, in order to be more targeted, only a few hundred messages are sent. The attacks are therefore more difficult to detect by monitoring tools and networks used by the authorities and monitoring operators. Therefore, fraud carried by e-mail cannot be solely identified and filtered by sensors, and e-mail accounts that are not owned by real individuals cannot be traced. Getting reports from real individual users who are the target of attacks has become critical.

The role of citizens is therefore crucial in evaluating and identifying online threats.

The Signal Spam database contains information useful to combat spam. Within this objective, data can be used for multiple purposes—civil or criminal—by public or private entities, to ensure the security of Signal Spam members or their customers. These include:

- LEA use for judicial investigations;
- Public use for data protection breach investigations;
- Securing network security for administration and government;
- Improving network security for, for example, Internet service providers;
- Improving the process of legitimate e-mail marketing;
- Brand and services protection;
- Facilitating e-mail delivery;
- Protecting clients' brands and services;
- Research.

## 2. Investigation

Close cooperation between law enforcement agencies and service providers is required in many areas and not only with regard to new, highly sophisticated online scams. Internet investigations create unique challenges that require the close cooperation between law enforcement agencies and providers.

One example is the international dimension of the network, since the process of transferring illegal content from one offender to another might involve a number of providers that

are often based in different countries. Tracing the route from one offender to another requires the close international cooperation between law enforcement agencies, as these investigations very often need immediate action.

### *Case study: eBay law enforcement portal*

eBay established the Global Law Enforcement Organization (GLEO) to promote the safe use of its platforms and to collaborate with local, federal and international law enforcement to help keep the community safe, enforce policies and prosecute fraudsters. Law enforcement agencies in North America seeking assistance and records for investigations relating to eBay and/or PayPal may contact the GLEO for assistance.<sup>49</sup> The Law Enforcement Portal enables authorized and verified law enforcement personnel around the world to request and access data owned by eBay electronically. Examples<sup>50</sup> of successful cooperation between eBay and law enforcement globally include:

- *Three arrested on stolen property charges*

Florida Department of Law Enforcement (FDLE) special agents recently arrested three people for leading a retail theft ring responsible for more than \$1 million worth of stolen Blu-ray DVDs from stores in Central Florida. Gregory Marinitz, 41, was charged with one count of dealing in stolen property, a first-degree felony, one count of organized scheme to defraud, a first-degree felony, and one count of dealing in stolen property by use of the Internet, a third-degree felony. James Davidson, 37, and Tina Pallay, 35, were both charged with one count of organized scheme to defraud. eBay, along with retail partners Barnes & Noble, Borders, Circuit City, and Target, assisted the FDLE in their investigation.

- *eBay joins forces to combat theft*

A major international grocery chain contacted eBay regarding the sales of various health & beauty and home improvement items by a particular seller on eBay. After review of the user's account, and with the assistance of the eBay retail partner, it was determined that the sellers were convicted retail thieves in the area. After concluding the investigation, eBay decided to take appropriate action per its policies and procedures. The case is currently being presented to law enforcement on behalf of the retail member and eBay.

- *Two arrested on ID theft charges*

Billy Morris Britt, 36, of Seattle, and Gabriel K. Jang, 37, of Renton, were arrested on charges of wire fraud and aggravated identity theft in November 2008. The suspects are accused of using stolen credit cards to buy computers and other electronic equipment, which was then sold for millions of dollars on eBay. They and others stole hundreds of credit cards from gymnasium lockers in Washington and Oregon, created nearly instant fake identification in their cars, and then purchased expensive electronics equipment with those stolen cards within hours of the theft. This equipment was then sold on eBay. A financial investigation showed that \$2 million from the sale of electronic goods had passed through a PayPal account

<sup>49</sup> [http://pages.ebay.com/securitycenter/law\\_enforcement.html](http://pages.ebay.com/securitycenter/law_enforcement.html) (last visited 10 January 2010).

<sup>50</sup> [http://pages.ebay.com/securitycenter/law\\_case\\_study.html](http://pages.ebay.com/securitycenter/law_case_study.html) (last visited 10 January 2010).

used by Jang since 2004, and another \$1.3 million into a checking account traced to Jang. eBay and PayPal investigators assisted the United States Secret Service in Seattle on an ongoing basis for over a year prior to the arrest.

- *UK man convicted in counterfeit scam*

Davut Turk, living in the United Kingdom, raked in tens of thousands of dollars selling expensive jewellery and ornaments on eBay over the past two years. Although described as silver, the products were actually made of brass. Turk's lucrative scam, which netted him approximately \$70,000, was exposed when a customer complaint led to raids on his home and a nearby storage locker. Mr Turk was recently convicted of 30 offences relating to trade descriptions and the use of counterfeit hallmarks. Officers found more than 200 pounds of fake silver items, ranging from rings and necklaces to candelabras and salt and pepper shakers. Turk was ordered to pay close to \$10,000 in court fees and fines. eBay and PayPal investigators assisted law enforcement in an ongoing basis over the course of several months. They were able to assist investigators trace the funds received for this scam as Mr Turk used PayPal to accept payment from his victims.

### 3. LEA training

An effective fight against cybercrime requires a carefully considered approach from industry and law enforcement. With the complexity and speed of development of new technologies such as new services being offered online for free, service providers are increasingly being asked to engage in a more active way in addition to responding to requests from law enforcement. Law enforcement agencies do not have the capacity to develop internally all the expertise that is required and cooperation with the private sector is not necessarily something done routinely. There are very few specific training programmes which address identity theft in isolation, since forensic analysis is common to all types of cybercrime activities.

Law enforcement agencies can gain and maintain an understanding of new technology areas from the Computer industry and Internet service providers. Industry and law enforcement agencies need to share their expertise and concerns.

Historically, there has been limited official cooperation between law enforcement and industry in the development of training and capacity building to combat the threat of cybercrime. Law enforcement agencies in different jurisdictions have traditionally developed their own training programmes and in some instances have worked with industry and academia in order to meet short term national objectives.

Since 2002, a coordinated effort has been made to harmonize cybercrime training across international, and in particular European borders. This has involved EU countries working together in pursuit of a concept developed in an EC FALCONE funded project entitled 'Cybercrime Investigation—Developing an International Training Programme for the Future'.

Organizations are constantly developing support services for new and existing personnel. As part of this, there is a need for training programmes for personnel to equip them with

the knowledge and skills necessary to ensure their work related skills and activities are matching international standards.

Closer collaboration between industry, law enforcement, academia and international organizations has been possible primarily through the formation of the Europol Working Group on the Harmonisation of Cybercrime Training. In addition, collaboration between Microsoft and Interpol has created a global law enforcement training programme coordinated by the International Centre for Missing and Exploited Children (ICMEC), based in Virginia, in the United States.

The economic downturn has emphasized the need to work in a smarter way and this study identifies ways in which the key partners in law enforcement, industry and academia can provide a more effective approach to delivering much needed training to law enforcement, provide a better return on available resources and also meet the needs of industry in developing their knowledge and skills in an environment that will also lead to appropriate qualifications.

### *Current initiatives*

#### **Law enforcement**

The Europol subgroup on the harmonization of cybercrime training born out of the successful European Commission funded projects is probably the best known example of the development of training programmes for the law enforcement community, created by collaboration between law enforcement, academia, industry and international organizations. The group has a five year plan for the development, maintenance and delivery of cybercrime training and qualifications. The current project has some 30 partners from these groups and is seeking further funding to develop more advanced training in line with the threats of cybercrime.

Interpol, through its five regional working groups, is delivering training and capacity building in all parts of the world. It is a partner in the Europol initiative and utilises the training material and other resources from the partners in the European project.

There is a strong working relationship between law enforcement and industry in the Asia Pacific region, with tools developed by industry being made available to law enforcement on a global basis. There are other joint initiatives that relate to specific investigations such as those involving botnets and facilities made available by industry to support law enforcement activities.

It does seem that most of the initiatives involve industry as donors and law enforcement as recipients. The study should identify whether it is possible for law enforcement to provide training to industry.

One area that has not been fully explored is the possibility of using the partnerships that may be developed to provide an investigative support capability to be taken advantage of in cases of major international cyber incidents. Traditionally law enforcement has tended

to focus on individual crimes, however, given the likely increases in incidents such as widespread denial-of-service attacks which recently occurred in Estonia, it might be useful to mobilize the corps of partners. This area is considered as relevant once the relationships have been formed to develop the training, education and research functions and is not dealt with any further in this paper.

Interpol, which has worked to train law enforcement officers around the world, has to date established various working parties on information technology crime in Europe, Asia-Pacific, Africa, North Africa/Middle East and the Americas regions. While much training has been given, it has been thus far on an ad hoc basis, and therefore not formally linked to any certification or qualification process. Many other multi-lateral organizations have also engaged in cross-regional training projects, including APEC, ASEAN and the OAS. As noted with Interpol, much of this training was ad hoc in nature and did not provide an ongoing level of instruction culminating in any official certification or qualification.

It is important that any proposed model for future cooperation takes account of the fact that many of the cybercrime threats posed to the European Union emanate from beyond the EU's borders. It is critical that European law enforcement officials build solid relationships with their counterparts in other regions of the world. Not only is this logical from an investigative and operational perspective, but also from a training perspective as well.

One such organization with whom cooperation might be desirable is the International Multilateral Partnership Against Cyber Threats (IMPACT), located in Kuala Lumpur, Malaysia. IMPACT has been designated by the United Nations' International Telecommunications Union as the key organization to implement the United Nations' Global Cyber Security Agenda and as such has responsibility for coordinating cybercrime and terrorism incidents in 191 countries around the world.

IMPACT has established a Global Cyber Response Centre to deal with real-time emerging cyber threats. In addition, it has a large academic network of over 20 universities spread across the globe conducting research on cyber security and assurance. While IMPACT is not specifically focused on the law enforcement community alone, it does provide a model to bring together law enforcement, regulators, governments, academic institutions and the NGO community to respond to the common threat posed by cybercrime and terrorism.

As part of the work proposed herein for the European Union, this study sought to identify appropriate partners such as IMPACT with whom we can cooperate in order to ensure that the work of the EU and other international initiatives is appropriately shared and harmonized across regions.

### University College Dublin, Ireland

It is now accepted that LE officers involved in cybercrime investigation around the world should be educated to the highest possible level. If possible, they should obtain formal accreditation for such education which enhances their standing when providing testimony in the courts.

In 1997, University College Dublin (UCD) helped to develop a one year Certificate in Forensic Computing and Network Security for the Irish Garda Computer Crime Investigation Unit to enhance their ability to combat technology related crime. This programme operated for three years and delivered targeted technical education to law enforcement personnel. UCD also provided *pro bono* expert assistance in criminal cases at a time when law enforcement agencies were establishing their skills in cybercrime.

In 2006, UCD established the UCD Centre for Cybercrime Investigation (UCD CCI) with the creation of a state of the art forensics laboratory and the development of a law-enforcement-only Masters Degree in Forensic Computing and Cybercrime Investigation (MSc FCCI).

The MSc FCCI was initially developed using the material created through the AGIS projects and was designed to address one of the goals of the initial FALCONE report that identified a requirement for advanced law enforcement qualifications in the field. To support ongoing education and training development, administration and delivery, the university currently provides funding for two full-time staff in the centre, as well as the ongoing use of the premises required to house the UCD CCI.

UCD's MSc in Forensic Computing and Cybercrime Investigation (MSc FCCI) is an accredited programme specifically designed in partnership with law enforcement. The programme is run on a not-for-profit basis and is currently restricted to law enforcement officers. The programme is being continually revised and updated in order to remain up to date in relation to cybercrime threats and makes constant use of research undertaken in the university to support content development.

Since its establishment, over 60 LE officers from 15 countries have graduated or are currently participating in the programme. The course is designed as an online learning programme to allow working professionals to learn in their own time and at their own pace.

In addition to supporting European and Europol initiatives, UCD Centre for Cybercrime Investigation participates as a member of the Irish Delegation to the INTERPOL Working Party on IT Crime—Europe. Membership of this group has led to the centre being asked to assist Interpol in a variety of ways:

- Interpol requested the UCD Centre to design a training programme that would support law enforcement officers in becoming trainers in their own right. This was a capacity building initiative that would facilitate the expansion of skilled cybercrime investigators in regions where they were most needed. UCD CCI has been requested by Microsoft and Interpol to act as validators for the COFEE forensics tool. Experts from CCI are currently testing the tool, and a training pack is in the process of being developed.
- In May 2008, UCD CCI was requested, and agreed, to provide expertise to participate in a meeting to review the outcomes of an operation conducted by Interpol in relation to the seizure of computers, belonging to the FARC terrorist group, by Columbian authorities.

- Interpol's collaborations with UCD CCI have led to the creation a Memorandum of Understanding between the two organizations to be finalized in April 2009. A further Memorandum of Understanding is to be completed between the International Multilateral Partnership Against Cyber-Threats (IMPACT) and the UCD Centre for Cybercrime Investigation.

UCD Centre for Cybercrime Investigation is also collaborating closely with the Organization for Security and Cooperation in Europe (OSCE), and is currently organizing a law enforcement training programme due to take place in Serbia later this year.

### Université de Technologie de Troyes, France

A specific collaborative effort has been undertaken in France that has led to a law enforcement/academic relationship. In 2001, the Gendarmerie Nationale launched at its "National Centre for Judiciary Police Training" (CNFPJ), in Fontainebleau, the first training of specialized investigators (who are called "NTECH" in the gendarmerie). This four-week training programme evolved over the years up to six weeks of training, covering high-tech legislation, investigations, forensic analyses of computers, mobile phones and smart cards as well as relations with industry.

Currently, industry is invited to participate in the NTECH training. This includes presentations by a French ISP, the three French GSM companies, the French ISP association and a French content producer (Canal+), etc. The feedback goes in both directions and these training sessions are very much appreciated.

Every year, the police and the gendarmerie organize a joint seminar for their specialized investigators (NTECH for the gendarmerie and ESCI for the police). Industry is regularly invited to make technical presentations.

In 2005, a partnership was signed with the Université de Technologie de Troyes to obtain academic accreditation of this training, which has now become a university diploma and covers a year of training—five weeks in class at the CNFPJ, three weeks in classes at the UTT and the rest of the year devoted to personal work and the preparation of a small thesis on a technical or investigative topic.

Since 2006, five selected among experienced "NTECH" have access each year to a master degree training at the UTT on information systems security (along with regular students). The objective for the gendarmerie is to train these personnel on matters they will encounter in medium to big corporate or public organizations' computer environments.

Both the university diploma and the master degree diploma have gained from this cooperation in terms of quality and content.

### European Union

The private sector and law enforcement are encouraged to assist each other with education, training and other support on their services and operations.



In 2001, the FALCONE project entitled “Training: Cybercrime Investigation—Building a Platform for the Future” was launched. This was a European Commission funded initiative that enabled a group of experts from LE and academia to meet, discuss and agree a set of recommendations for the future shape of cybercrime investigation training. The UCD Centre for Cybercrime Investigation became involved as a partner.

This was followed by the AGIS 2003–2006 projects. These projects implemented the recommendations of FALCONE by developing accredited modularized European training programmes for LE. The UCD Centre for Cybercrime Investigation supported these projects through the provision of content experts, academic oversight and accreditation, course trainers, hosting of meetings and development of final report recommendations.

A further FALCONE success was the creation of a Europe-wide working group that would continue to promote and develop harmonized training programmes for law enforcement and the Europol Cybercrime Investigation Training Harmonization Group, formed in 2007, fulfils this role. (UCD CCI has been a member and provided *pro bono* support since its inception.) The group currently has two major initiatives scheduled for 2009; the upgrade of the existing training programmes and the three-year ISEC project, under which 30 law enforcement officers will graduate from UCD with a Masters in Forensic Computing and Cybercrime Investigation.

The upgrade project is being jointly managed by staff from the UCD Centre for Cybercrime Investigation and the German Police. UCD has taken responsibility for the financial administration of the project, will host a number of the meetings, and also provide a training designer for all upgrades.

Microsoft has partnered with Interpol, the EU, universities and 15 EU member States to help fund the AGIS projects which emphasizes cooperation among public and private entities in fighting cybercrime. The project promotes standardized training programmes and information networks across participating countries. The AGIS project came to its conclusion, and its successor is ISEC, under the new programme “Prevention of and Fight against Crime as part of the general programme Security and Safeguarding Liberties”. Microsoft is working to participate in this new programme.

### 2CENTRE EC-funded project

A Cybercrime Centres of Excellence Network for Training Research and Education (2CENTRE) will enable the production and dissemination of accredited training courses to fit within a structured and sustainable framework. The programme supports the strategy and peer programme of the European Commission explained in its last communication paper “Towards a general policy on the fight against cybercrime” COM(2007) 267 dated 22.05.2007, in which one of the aims is the need to set up a coordinated action to train law enforcement in this area. The project also recognizes that there are those in the industry sector tasked with combating cybercrime and do not have access to the training and education programmes previously developed. Industry, law enforcement and academia are the three key players in this project, and national centres will be developed within this tripartite collaboration. Industry cybercrime professionals will have the opportunity to

participate in training and education programmes alongside their law enforcement counterparts, and to aid the development of new training modules and education programmes. Another key feature of the project is research into cybercrime and the development of software tools. Opportunity for different centres to work together towards common aims is envisaged.

The project will commence with two national centres in France and Ireland, and will create a coordination centre whose work will include the development of terms of reference for the network, common procedures respecting the national legal and cultural background of current and future network partners, develop methodologies for commissioning, quality control and other associated activities.

Each national centre will work on its own list of projects agreed by the partners. The projects will aim to enhance the capability of combating cybercrime in the EU and beyond. Each component of the project will have an advisory board which will give clear direction.

The project will use meetings, exchange visits, and resources such as websites for use with the project team and with interested parties. Each separate project within the overall programme will have its own project plan, timetable and project team. Progress will be monitored at regular intervals by the individual advisory boards and the coordination centre. The 2CENTRE concept and plans will be delivered at relevant conferences and seminars to gain support and new members.

The EC-funded project will produce terms of reference, good practice and common procedures for the running of and recommendations for the future of 2CENTRE. Agreement with Europol for sharing the training material, a fully functioning website for the project, a number of training modules on CD to be made available to all partners of the 2CENTRE project, forensic software tools ready for use, tool validation documentation, instruction manuals/training packs for each tool, publication of reports for dissemination and use by 2CENTRE partners, development of e-learning courses, IP specifications for parties involved, enhancement of existing training and education programmes, translation of a number of modules and product brochures into other languages.

## Council of Europe

In order to counter cybercrime and protect computer systems, governments must provide for:

- Effective criminalization of cyber-offences. Legislation of different countries should be as harmonized as possible to facilitate cooperation.
- Investigative and prosecutorial procedures and institutional capacities which allow criminal justice agencies to cope with high-tech crime.
- Conditions facilitating direct cooperation between state institutions, and between state institutions and the private sector.
- Efficient mutual legal assistance regimes, allowing direct cooperation among multiple countries.

The Convention on Cybercrime (ETS 185) of the CoE helps countries respond to these needs. It was opened for signature in November 2001 and by December 2008 had been ratified by 23 and signed by another 23 countries. The Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189) of January 2003 had been ratified by 13 and signed by another 21 States. Equally important is that a large number of countries worldwide is using the convention as a guideline or model law for the strengthening of their cybercrime legislation.

In order to support countries worldwide in the implementation of this treaty, the Council of Europe in 2006 launched the Project on Cybercrime ([www.coe.int/cybercrime](http://www.coe.int/cybercrime)) which was funded from the budget of the Council of Europe and contributions from Estonia and Microsoft. Phase 2 of this project will start in March 2009 and last until June 2011.

Under this project, the Council of Europe supports training on:

- Cybercrime legislation;
- International police and judicial cooperation;
- Law enforcement—service provider cooperation;
- The prosecution and adjudication of cybercrime offences;
- 6-10 December 2009, Egypt—training for judges on cybercrime/electronic evidence, including online child abuse.<sup>51</sup>

### Simon Fraser University (SFU) International Cybercrime Research Centre, Canada

A new research centre to fight cybercrime is established at SFU's Surrey campus, with a \$350,000 grant from the provincial government. The centre is a joint venture of SFU, the province, and the International Society for the Policing of Cyberspace (POLCYB), a British Columbia based non-profit organization established to prevent and combat crimes on the Internet. The International Cybercrime Research Centre will investigate online crime trends and help to develop new tools to counter cybercrime. As one of its initial projects the centre plans to develop virus scanner-like tools to detect child exploitation images.

SFU will bring cross-disciplinary expertise in computing science, engineering, and criminology to the new centre, with the statement that "There is no university in North America I'm aware of with a dedicated cybercrimes studies programme," Huge demand is expected at the graduate and undergraduate levels, as well as professional studies certificate courses through continuing studies.

### United Nations

The United Nations Office on Drugs and Crime has been developing a project entitled "Establishing and strengthening legal and policy frameworks to address cybercrime in developing countries".

<sup>51</sup> [http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default\\_en.asp](http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp) (last visited 10 January 2010).

The proposed framework, which will target developing countries, is comprehensive and will draw on the expertise and experience of those partners already active in the field. It aims at fighting computer-related crimes in four ways:

- Assist Member States in the adoption of adequate legislation that would constitute a solid basis for effective investigation and prosecution of computer-related crimes;
- Build the operational and technical knowledge of judges, prosecutors and law enforcement officials on issues pertaining to cybercrime;
- Train the judicial profession to effectively use international cooperation mechanisms to combat cybercrime;
- Raise awareness of civil society and create momentum among decision-makers to coalesce efforts to prevent and address cybercrime.

The key aspect for the purposes of this paper is the second objective, which reflects the work currently being carried out by a number of the other initiatives. UNODC is a full member of the Europol Working Group on the Harmonization of Cybercrime Training and will directly benefit from the creation of the proposed network of Centres of Excellence.

UNODC is also partnering with the Korean Institute of Criminology to develop a virtual cybercrime forum which will provide training and research. Industry is also involved as a partner of this project and provides funding for the infrastructure for the forum.

### International Center for Missing and Exploited Children/Interpol/Microsoft

The Computer Facilitated Crimes Against Children training seminar was designed to provide law enforcement around the world with the tools and techniques to investigate Internet-related child exploitation cases. This initiative was launched in December 2003 at Interpol Headquarters in Lyon, France. As of November 2008, a total of 3,221 law-enforcement officers from 113 countries have been able to participate in 36 regional training sites in France, Costa Rica, Brazil, South Africa, Croatia, Hong Kong SAR, Romania, Spain, Jordan, Argentina, Russian Federation, New Zealand, Thailand, Turkey, Japan, Norway, China, Bulgaria, Australia, Oman, India, Lithuania, Morocco, Qatar, Panama, Philippines, Poland, Peru, Czech Republic, Greece, Ukraine, Republic of Korea, Egypt, Brazil, Colombia and Italy.

The four-day seminar includes the following modules:

- Computer facilitated exploitation of children;
- Conducting the online child abuse investigation;
- Managing the law enforcement response to computer facilitation crimes against children;
- Prosecuting the offender;
- Technical aspects of the investigation;
- Resources and guest speakers.

The financial underwriting sponsor of the training initiative is offered an opportunity to actively participate in this portion of the training. The curriculum is also modified to complement the needs of the host country (i.e., culture, legal, linguistic, law enforcement, etc.).

In addition, ICMEC is now managing the operational role of CETS (Child exploitation Tracking System developed by Microsoft) to assist cybercrime investigations.

ICMEC is also part of the financial coalition, where they are working with the financial services industry to create a mechanism to report cases of illegal transactions such as online purchase of child pornography and provide training to law enforcement agencies on this mechanism.

### Industry initiated

The French Internet Access and Service Providers Association (AFA) has been involved since 2003 in training sessions about cooperation between ISPs and LEA, organized by the NTEC (specialized investigators in high-tech crimes) and the French National School for the Judiciary.

In August 2006, Microsoft has launched a website portal for law enforcement authorities around the world. The Law Enforcement Portal ([www.microsoftlawportal.com](http://www.microsoftlawportal.com)) is designed to provide law enforcement with easy access to training material and resources related to cybercrime. This portal is a response to the growing volume and variety of requests from law enforcement to Microsoft, related to its software, game or online services. The materials include summaries of various online threats—including children's safety, phishing, spyware, spam, and malicious code—and information about organizations, partnerships, and other resources available to help law enforcement understand, investigate, prevent, and address these threats.

In December 2004, Microsoft announced the Digital PhishNet (DPN), an alliance between law enforcement and industry leaders in a variety of sectors including technology, banking, financial services, and online auctioneering. This alliance is directed specifically at sharing information in real time about phishers to assist with identification, arrest, and prosecution. DPN is the first group of its kind to focus on assisting law enforcement in apprehending and prosecuting those responsible for committing crimes against consumers through phishing.

It provides a neutral, confidential and collaborative forum between the private and public sectors where information about instances and trends of phishing and related cyber-threats can be shared in confidence, analysed, and referred to law enforcement and various anti-phishing services, leading to aggressive enforcement and deterrence of future online offenses. It is managed by National Cyber-Forensics & Training Alliance (NCFTA), a non-profit public/private organization in the United States, with staff from both law enforcement and industry. NCFTA provides training and support for LE; it connects law enforcement with industry experts for analysis and forensics. NCFTA is funded and supported by its members. DPN is organizing closed meetings between industry and law enforcement to facilitate cooperation. After Chicago in 2005 and New Orleans in 2006,

DPN expanded to Europe with Berlin in June 2007 and to Asia with Singapore in January 2008. It met again in the United States in San Diego, California, in September 2008.

Microsoft has developed materials to help law enforcement officials understand the ways in which available technology and software can be used to investigate cybercriminals. These materials include information relating to the technical details of Microsoft's products and guidance for conducting investigations on computers and other devices using Microsoft software.

In October 2006, Microsoft has hosted the "LE Tech 2006" conference at Microsoft headquarters in Redmond, Washington. Gathering around 300 international law enforcement officers from over 45 countries, the event has introduced law enforcement officers from around the world to Microsoft's newest efforts to assist in cybercrime investigations, including the Child Exploitation Tracking System (CETS), Microsoft's new Law Enforcement Portal, and Microsoft's enforcement programmes.

In January 2008, Microsoft and eBay/PayPal/Skype provided five day training to more than 40 experienced computer related crime investigators from the European Union Member States on malware and botnets. In June 2006, Microsoft organized with Europol a 4 day training course for 24 high-tech crime investigators from 15 member countries and in addition 12 people from Europol High Tech Crime Center and other specialized units of Europol. The training covered advanced Windows XP Forensics above and beyond what the available tools cover, MS Office metadata and hiding techniques, botnet malware detection and analysis, Windows Vista security preview and demo, as well as the ICI team's response to the malware threat. Access was granted. Microsoft Windows Vista BETA was also discussed.

With regards to training, Microsoft sponsors or hosts training around the world with regards to a variety of threats, capacity building and child protection. Examples include:

- The International Botnet Taskforce (IBTF) started in 2004 and is an annual meeting where international law enforcement, industry partners, security researchers, and private companies can come together to discuss ways in which this community can work together to curb the threat of botnets. This series of conference is seen as one of the premier of its kinds and the participants are of the highest calibre in their respective fields. The eighth IBTF meeting took place on 21 October 2008 in Arlington, Virginia (United States). With representatives from almost 40 countries and close to 200 attendees, this meeting represented one of the broadest selections of attendees in the 4 year history of the conference, combining participants who came for the first time and members that have been involved from the beginning.
- Law Enforcement Tech 2006 and 2008 (LE Tech): LE Tech was an intensive three-day training designed to equip law enforcement with the latest technology tools and information for cybercrime investigations. The conference focused on technical details and "know-how" around Microsoft's latest products and services.

Through LE Tech and similar trainings, Microsoft has helped train over 6,000 law enforcement officers from over 110 countries (including 1,500 in the United States) around the world and is able to provide the necessary tools and skills to identify cybercriminals.

Initiatives taken by eBay include:

- The Nigerian Economic Financial Crimes Commission.
- Training of 60 criminal judges/prosecutors organized by Berlin Senate of Justice.
- A joint training session/conference conducted by eBay, CBI and Interpol for Top 350 law enforcement officials in India.
- Training of the majority of detectives within the United Kingdom's Serious and Organized Crime Agency (SOCA) throughout the year.
- National Magistrates Institute, Bucharest, Romania, "Train the Trainers" session for two groups of judges and prosecutors, either through organized programmes at eBay UK or through outreach at their forces or local offices.
- In 2009, training of more than 1,700 law enforcement officers from around the United Kingdom.

#### Interesting eBay statistics

- 85 million+ active users worldwide
- \$2000 traded every second
- 110 million+ active listings at any given time
- 1,500 cars sold on eBay every day
- 12,000–13,000 pairs of shoes sold every day

Presentation at the OSCE National Expert Workshop on a Comprehensive Approach to Cyber Security on 23–24 November 2009 by Tiberius Rusu, eBay Europe.

eBay fraud investigation training topics include:

- Introducing eBay's Fraud Investigation Team (FIT);
- Understanding fraud practices;
- Fraud investigation case studies;
- Interacting with eBay's Fraud Investigation Team;
- Submitting DPA requests;
- Urgent requests;
- Potentially available evidence and tips on what to ask for;
- Understanding the evidence supplied;
- Requesting witness statements;
- Requesting live court testimony;
- Overview of eBay's law enforcement page;

- Law Enforcement Portal;
- Qualifying criteria;
- User search fields;
- Search limitations;
- Conducting covert investigations.

### *Other*

There are a number of cybercrime training programmes being conducted by European law enforcement agencies, often through national training centres. These are primarily for law enforcement. In addition there are programmes that allow both law enforcement and industry delegates.

Several of these latter offerings are arranged by not-for-profit organizations such as the High Tech Crime Investigators Association (HTCIA) and the International Association of Criminal Investigators Association (IACIS), which both emanated from the United States and have international chapters. There are well known training programmes that are open to both industry and law enforcement, perhaps the best known of which is the SANS Institute in the United States.

### *Currently available training activities*

The IT Forensic and Cybercrime Investigation training activities that are currently available to law enforcement fall into a number of categories:

- National and regional training programmes such as those in the United Kingdom, Belgium, Germany, Canada, United States and France, to name but a few;
- Invited international guests to the above programmes;
- Training workshops held at cybercrime conferences;
- Training delivered by international police organizations such as Interpol and Europol;
- Industry training initiatives to support law enforcement activity;
- Software and hardware vendors;
- Training initiatives developed by national governments and/or international organizations;
- Training cascaded by those having attended one or more of the above initiatives;
- Training available as a result of initiatives such as the EC funded FALCONE/Agis/ISEC programmes;
- Training on cybercrime legislation by Council of Europe, United States Department of Justice, the Organisation of American States and others.



Historically, training has been developed in isolation with little collaboration. It was for this reason that the original FALCONE cybercrime training programme was created. Many countries and organizations were found to be developing almost identical training modules. This was seen to be a waste of scarce resources and the concept behind the project was to create a framework that would enable training to be developed collaboratively and delivered and made available free of charge to law enforcement on a global basis.

There are currently seven such courses that have been piloted and made available. These have been translated into a variety of languages, included in national training programmes and delivered in many parts of the world. There is, however, no coordinating body to ensure quality standards are maintained and that course material is current and where translated, made available to as wider audience as possible. The role of distribution of the materials currently rests with Europol for Europe and Interpol for the rest of the world. There is no campaign to market the availability of the material.

There have been other attempts in the past to attempt to coordinate training activity; such as the International Cybercrime Training Action Group (ICTAG), an initiative of the Canadian Police College and involving cybercrime training centres from a number of English speaking countries. This and similar initiatives were not successful as they had no full time resource devoted to looking after the activities of the group. This is another example of why network coordination is required for any international solution.



# VI. LIMITS OF COOPERATION

## 1. Legal limitations

Public-private partnerships have their limits in effectiveness.

### *Data protection legislation*

Since no party in the relationship can take steps which would breach the law, there are significant challenges when the sharing of information requires changes in legislation in order to permit that exchange. This exchange depends on the nature of the data concerned and the legislative environment to which that data and the exchange are subject.

During a fraud investigation, law enforcement agents often require access to large amounts of data in relation to customers who might be involved with or related to an online criminal activity especially relating to identity fraud and economic crime. This data is owned by an Internet service provider who might be hosting this data in the country where the investigation takes place or in a different location. For example, eBay have an eBay Privacy Policy Appendix—Data Sharing,<sup>52</sup> where they clearly outline which data will be given to third parties.

Type of information	Property rights owners (VeRO) members	Internal service providers	Public view	Users in a transaction	Law enforcement and government agencies
<b>Contact information</b>					
Full name	Yes	Yes		Yes	Yes
User ID	Yes	Yes	Yes	Yes	Yes
E-mail address	Yes	Yes		Yes	Yes
Street address	Yes	Yes		Yes	Yes
State	Yes	Yes	Yes	Yes	Yes
City	Yes	Yes		Yes	Yes
Zip code	Yes	Yes		Yes	Yes
Telephone no.	Yes	Yes		Yes	Yes
Country	Yes	Yes	Yes	Yes	Yes
Company	Yes	Yes		Yes	Yes
... 14 other items in this category					

<sup>52</sup> <http://pages.ebay.com/help/policies/privacy-appendix.html> (last visited 10 January 2010).

<b>Financial information</b>	
	7 items in this category
<b>Shipping information</b>	
	5 items in this category
<b>Transaction information</b>	
	7 items in this category
<b>Computer generated data</b>	
	10 items in this category
<b>Miscellaneous</b>	
	3 items in this category

It is excellent that this detailed list of stored data is published transparently by eBay. It is worth noting that eBay lists 27 companies around the world that are members of the Internet service providers—all of which will have access to the full dataset.

### *Competition law*

Competition law can be a real problem when all industry players work closely together to create a common standard or common response to specific market conditions. Great care needs to be taken to ensure that whatever steps are implemented are legally and financially possible by all market players and cannot be interpreted as behaving as cartel. For example, during the negotiations about the code of practice for the Internet industry<sup>53</sup> in Ireland, there were extended discussions about how Internet service providers should handle customers who misbehaved in using one supplier and then moved to another supplier. There were restrictions how Internet service providers could share such information due to data protection and competition law.

The EC competition rules are contained in the Treaty of Rome, especially in Articles 81 and 82.<sup>54</sup>

#### *Article 81 (ex 85) EC*

Article 81(1) EC prohibits agreements, concerted practices, and decisions of undertakings which may affect trade between member States and which have as their object or effect the prevention, restriction, or distortion of competition. Article 81(2) EC provides that any such agreements or decision are automatically void. Article 81(3) provides that the Commission (and the Commission alone) may declare the prohibition in Article 85(1) inapplicable if certain requirements are met.

#### *Article 82 (ex 86) EC*

Article 82 prohibits the abuse of a dominant position within the common market or a significant part of it, in so far as it may affect trade between Member States.

<sup>53</sup> <http://www.ispai.ie/docs/percent5Ccope.pdf> (last visited 10 January 2010).

<sup>54</sup> [http://en.wikipedia.org/wiki/Treaties\\_of\\_Rome](http://en.wikipedia.org/wiki/Treaties_of_Rome) (last visited 10 January 2010).

### *Article 86 (ex 90) EC*

Article 86 EC confirms that activities of public undertakings and undertakings to which member States grant special or exclusive rights are also subject to the competition rules of the Treaty. Article 86 provides there should be no state protected monopolies unless such monopolies are in the public interest.

### *Human rights*

Sharing information and data between government and law enforcement parties can be a challenge in some countries of the world where the rule of law and democratic principles are not always followed. Human rights is a key issue to consider when public-private partnerships create what are in essence closed non-transparent environments for sharing of sensitive information. It is critical therefore that such environments consider issues of transparency and accountability perhaps by regular reporting or by putting in place a public oversight mechanism. An advisory board could provide oversight and guidance of the strategy of the partnership.

### *Cosy relationships*

When key stakeholders, which include governments, Internet service providers and law enforcement agencies, agree to a regular exchange of information and to formulate policies to ensure efficiency in the investigation of crime, there can be times when such relationships might be seen to be unbalanced and not in the long term interests of a transparent accountable democracy.

One national reaction to such as initiative is described in an article in the *Irish Times* of 25 September 2009, with the headline “Startling memo on retaining data”. Journalist Karlin Lillington wrote:

A “private” data-retention agreement is based on sweeping assumptions, not articles of law. A secret memorandum of understanding between State agencies and the communications industry on how to implement the as-yet non-existent government data retention legislation, confirms longstanding concerns about who is managing the data retention agenda and to what end.

With data retention, it appears that the tail is wagging the dog, in blatant disregard for proper democratic legislative process. The agencies that want access to our call and Internet data are bypassing the Oireachtas, which at least theoretically, is the body that draws up and implements legislation.

As one alarmed privacy advocate told me: “This is legislation by decree”. The “Memorandum of Understanding (MoU)”, seen by the *Irish Times*, is dated 17 August and was drawn up “between the Communications Industry and the following State agencies: the Commissioner of An Garda Síochána, the Permanent Defence Forces and the Revenue Commissioners”, as stated in the opening paragraph of the memorandum.

The article received a number of responses in the *Irish Times* of 2 October 2009:<sup>55</sup>

Rossa McMahon stated that:

It is notable, however, that her latest report, on a secret deal between State agencies and telecommunications companies to share more data with the State than they will be required to by law is buried in the business section (*Business This Week*, 25 September). This secret deal is not just startling, it is shocking, even if we are no longer surprised by secretive State deals.

Ronan Lupton, Chairman, Alternative Operators in the Communications Market (ALTO); Paul Durrant, General Manager, Internet Service Providers Association of Ireland and Tommy McCabe, Director Telecommunications and Internet Federation representing the Irish Internet and telecommunications industry responded that:

This draft memorandum is highly desirable as it also aims to establish a single point of contact principle which should minimize mistakes and abuse. There is nothing “secret” about the memorandum, it is simply at a stage where it is still being negotiated and not public.

It is critical that any public-private partnership which aims to fight crime in society or on the Internet includes a range of organizations including those responsible for data protection, human rights, etc.

## 2. International restrictions

There are a range of international restrictions which are not always adopted by public-private partnerships. Information sharing across national boundaries relating to data which might have national security implications can prevent or disrupt such sharing. Investigations which require evidence which can be used in a court case need to be implemented in line with such strict requirements for a “chain-of-evidence”.

## 3. Limits on capabilities

There are limits on what organizations can do for a variety of reasons.

### *Business competition*

Many of the key business stakeholders operate in competition with each other. They come together to focus on common concerns in society and on issues which at one time or another are considered major competition issues. For example, some companies strive to project a family friendly image through the services they offer and through their marketing

<sup>55</sup> <http://www.irishtimes.com/newspaper/letters/2009/1002/1224255674433.html> (last visited 10 January 2010).

and advertising activities. The home market is a key market which they believe is motivated by safety, security and trust. Having substantial market knowledge at considerable cost and time, and unique business knowledge gained in how to satisfy this core market, there can be a real threat to this business model in a shared public-private partnership which aims to facilitate and enable these skills across the complete market.

### *Legal restrictions on sharing*

Many law enforcement agencies have significant institutional or legal restrictions on sharing information with non-law enforcement agencies, and this can restrict the range of relationships and partnerships into which they can enter.







# VII. CONCLUSION

## 1. What works

Public-private partnerships as a response to crime both online and offline provide the most effective response to complex criminal activity today, especially in the area of identity theft and economic crime.

### *Knowledge and skills sharing*

They bring together a range of knowledge, skills and experience from diverse backgrounds such as industry, government, human rights, law enforcement and the legislature, which increases the overall effectiveness of the partnership since organizations who would normally operate alone can never cover all these issues. Each partner organization holds information and knowledge which, if shared, can provide a more complete view of the criminal activity and in some cases can provide evidence which can be used in court cases. Working together ensures minimum duplication of effort, high quality sharing and research, shared with others in the network to ensure consistency and scalability compatible with cultural and linguistic sensitivity.

### *Independent coordination*

Public-private partnerships create a need for independent coordination. Without such coordination international cross-coordination is limited and relies on a few individuals to drive the activities. Proper organized and dedicated coordination is required in order to encourage sharing, expand the partnership to new organizations and new countries as appropriate, support external relationships with transnational agencies and activities and promote the work of the partnership. Funding is often a major problem for such coordination centres and they require broad long term financial and advisory support in order to be sustainable.

## 2. What doesn't work

Partnerships which are based on unequal sharing, unequal levels of power or which are not based on mutual respect and understanding will find working together fraught with problems and challenging. Crisis events will cause divisions and marginalisation unless clear

roles and relationships are defined. It is a mistake to consider that such public-private partnerships on their own will solve all problems relating to identity theft. There is a need for updated legislation, international initiatives, international coordination of law enforcement and agreed industry self-regulation and codes of practice.

### 3. What will happen next


- Public-private partnerships need support and encouragement.
- Sustainable international coordination of such partnerships is a major challenge.
- New generations of online malware are getting more and more sophisticated. Botnets are very flexible and used for multi-purposes such as to make money (rent, extortions, industrial espionage etc.), to steal personal and financial data, to boost social engineering (phishing and its varieties), to perpetrate huge spamming, to threaten the victim and to attack critical information infrastructures networks. The peril is coming from everywhere and prevention is difficult.<sup>56</sup>

---

<sup>56</sup> *Mr Nicole Dilone*, “European Alert Platform”, High Technology Crime Centre, Europol, at the Public-Private Dialogue to Fight Online Illegal Activities hosted by the European Commission in Brussels, 27 November 2009.





A magnifying glass is positioned over a fingerprint, which is partially visible. In the background, there is a blurred image of an ID card or membership card. The card shows some text, including 'JAMES B. SMITH', '0324', '3954', 'VALID THRU 07/09', and 'BLADE MEMBER'.

# PRACTICAL GUIDE TO INTERNATIONAL COOPERATION TO COMBAT IDENTITY-RELATED CRIME\*

**Marco Gercke**  
**Raluca Simion**

---

\*This Guide was prepared by Dr Marco Gercke and Dr Raluca Simion on behalf of the United Nations Office on Drugs and Crime (UNODC) and in compliance with the recommendations of a core group of experts on identity-related crime, established by UNODC to pool experience, develop strategies, facilitate research and agree on practical action against identity-related crime. Further information on the work of the core group can be found at: <http://www.unodc.org/unodc/en/organized-crime/index.html?ref=menuseide>.



## Contents

	<i>Page</i>
I. INTRODUCTION .....	239
1. Aim of the guide .....	239
2. The development of identity-related crime.....	239
3. Impact of the digitalization on the transnational nature of the offence .....	241
4. Extent of organized crime involvement .....	242
II. GENERAL ASPECTS OF INTERNATIONAL COOPERATION IN IDENTITY-RELATED CRIME CASES .....	245
1. Importance of international cooperation in combating identity-related crime .....	245
2. Main instruments with reference to the international cooperation in combating identity-related crime .....	246
III CONVENTIONS APPLICABLE IN INTERNATIONAL JUDICIAL COOPERATION IN COMBATING IDENTITY-RELATED CRIME AND PRACTICAL ISSUES EMERGING FROM THEIR APPLICATION .....	263
1. Importance of identifying the applicable instrument.....	263
2. Conventions applicable with regard to the extradition procedure .....	264
3. Conventions applicable with regard to traditional forms of MLA .....	273
4. Specific forms of mutual legal assistance provided through the Council of Europe Convention on Cybercrime and the Harare MLA Scheme which can be relevant in identity-related crime.....	294
5. The role of networking in solving the MLA requests .....	297
IV. CASES .....	303
1. First case—cloned credit cards .....	303
2. Second case—“phishing” .....	306
3. Third case—auction fraud.....	308
4. Fourth case—account takeover.....	312
5. Fifth case—skimming .....	314
6. Sixth case—skimming II .....	320
7. Seventh case—smuggling of migrants .....	323
8. Eighth case—forgery.....	325
9. Ninth case—counterfeit documents/trafficking in persons.....	329
10. Tenth case—Joint Investigation Team (JIT)/trafficking of persons.....	332
11. Eleventh case—Internet-related offence .....	334





# I. INTRODUCTION

## 1. Aim of the guide

Given the largely transnational dimension of identity-related crime, international cooperation in criminal matters is highly relevant for the success of many investigations. As there are significant differences between national investigations and investigations requiring the use of instruments of international cooperation, the present guide intends to provide an overview of aspects pertaining to the transnational dimension of identity-related crime (1) and the general principles of international cooperation (2). To facilitate investigations, this guide also provides an overview of some of the most relevant case examples (3). Due to the complexity of the subject matter, the guide focuses on basic information and guidelines on how to best deal with international cooperation requests in the field of identity-related crime.

## 2. The development of identity-related crime

The wide media coverage,<sup>1</sup> the results of various surveys analyzing the extent and loss caused by identity theft,<sup>2</sup> as well as numerous legal and technical analyses<sup>3</sup> published over the last years, could easily lead one to the conclusion that identity-related offences are a 21st century phenomenon.<sup>4</sup> This is certainly not the case. Offences such as impersonation, falsification and misuse of identity documents are known for more than a century.<sup>5</sup> Already in the 1980s, the press reported widely on the misuse of identity-related information.<sup>6</sup>

The increasing use of digital information, however, opened new possibilities for offenders to get access to identity-related information.<sup>7</sup> The transformation process from

<sup>1</sup> See, for example, *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: <http://edition.cnn.com/2006/US/05/18/identity.theft>; *Stone*, U.S. Congress looks at identity theft, *International Herald Tribune*, 22.03.2007, available at: <http://www.iht.com/articles/2007/03/21/business/identity.php>.

<sup>2</sup> See, for example, 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

<sup>3</sup> See, for example, *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, *Lex Electronica*, vol. 11, No. 1, 2006; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, *MMR* 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000.

<sup>4</sup> *Hoar*, Identity Theft: The Crime of the New Millennium, *Oregon Law Review*, vol. 80, 2001, page 1421 et seq.; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, *British Journal of Criminology*, 2008, page 8.

<sup>5</sup> See Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, page 5.

<sup>6</sup> See *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003, page 1.

<sup>7</sup> *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, *Crime, Law and Social Change*, vol. 46, page 270.

industrialized countries to information societies<sup>8</sup> had a particularly large impact on the development of identity theft-related offences. Despite the large number of Internet-related identity theft cases, digitalization did not fundamentally change the offence itself, but, instead, created new targets and facilitated the development of new methods of crime.<sup>9</sup> However, despite the trend toward online identity-related crime, offline crimes remain dominant.<sup>10</sup> Less than 20 per cent of the offences that could be categorized in the United States in 2007<sup>11</sup> were online-related scams and data breaches.<sup>12</sup>

The remaining importance of offline crimes is surprising as the digitalization and moreover the globalization of network-based services led to an increasing use of digital identity-related information. Major sections of business as well as federal operations depend on the processing of electronic data by automated systems.<sup>13</sup>

Identity-related information is of growing importance in the economy as well as in social interaction. In the past, a “good name” and good personal relations dominated business as well as daily transactions.<sup>14</sup> With the transfer to electronic commerce, face-to-face identification is rarely possible, and, as a consequence, identity-related information became much more important for participation in social and economic interaction.<sup>15</sup> The process of “instrumentalization”,<sup>16</sup> whereby an identity is translated into quantifiable identity-related information, is of great significance, as is the distinction between, on the one hand, identity of a person defined<sup>17</sup> as the collection of personal characteristics, and on the other, the quantifiable identity-related information which enables the recognition of a person.

Nowadays the requirements of non-face-to-face transactions, such as trust and security,<sup>18</sup> dominate the economy in general, and not just e-commerce businesses. An example is the use of payment cards with a PIN (personal identification number) for purchasing goods in a supermarket. Having access to identity-related information enables the offenders to participate in wide areas of social life. Apart from this, the fact that this information is not only processed but, in general, also stored in databases, makes those databases a potential target for offenders.

<sup>8</sup> For more information on the information society, see *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

<sup>9</sup> *Clarke*, Technology, Criminology and Crime Science, *European Journal on Criminal Policy and Research*, vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 51; Identity Fraud, Prevalence and Links to Alien Illegal Activities, GAO, 2002, GAO-02-830T, page 6, *Paget*, Identity Theft, McAfee White Paper, 2007, page 6; For an overview about Internet-related phishing see: *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, pages 8 et seq.

<sup>10</sup> 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, page 5.

<sup>11</sup> 35 per cent of the overall number of cases.

<sup>12</sup> 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy and Research, page 6.

<sup>13</sup> Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07\_935T, page 4.

<sup>14</sup> *Elston/Stein*, International Cooperation in On-line Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: <http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf>.

<sup>15</sup> See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, *Datenschutz und Datensicherheit*, 2006, page 555.

<sup>16</sup> *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, *Bulletin of Science Technology Society*, 2007, vol. 27, 2008, page 20.

<sup>17</sup> See *Encyclopaedia Britannica*, 2007.

<sup>18</sup> *Halperin*, Identity as an Emerging Field of Study, *Datenschutz und Datensicherheit*, 2006, page 533.

### 3. Impact of the digitalization on the transnational nature of the offence

The increasing number of Internet-related cases has significant impact on the work of investigators, as Internet-related crimes are, to a large degree, transnational in nature.<sup>19</sup> The Internet was originally designed as a military network<sup>20</sup> based on a decentralized network architecture. As a consequence of the underlying digital architecture, as well as the global availability of services, cybercrime often has an international dimension.<sup>21</sup> E-mails with illegal content easily pass through a number of countries during the transfer from sender to recipient. Even if sender and recipient are both located in the same country, the case can have a transnational dimension if just one of them uses an e-mail service operated by a provider outside the country. Taking into account that some of the popular free e-mail services have several hundred million users, it is obvious that cybercrime, by its very nature, often has a transnational dimension.<sup>22</sup>

The transnational dimension of Internet-related cases can be underlined by referring to statistics about the location where “phishing” websites are stored. In May 2009, the Anti-Phishing Working Group listed the following countries: United States (68 per cent), China (6 per cent), Canada (6 per cent), Germany (2 per cent), United Kingdom (1 per cent) and Sweden (1 per cent).<sup>23</sup>

The consequences for investigation of cybercrime are similar to other dominantly transnational offences: the fundamental principle of national sovereignty does not permit investigations within the territory of foreign countries without the permission of local authorities.<sup>24</sup> Therefore it is crucial for cybercrime investigations to ensure close cooperation of the countries involved.<sup>25</sup>

A major difference from other areas of transnational crime is that the time slot available in cybercrime investigations is often narrow. Unlike drug trafficking, where—depending on the means of transportation—it can take weeks before narcotics reach the recipient, an e-mail can be delivered within seconds and (with an adequate bandwidth) even large files can be downloaded within minutes.

<sup>19</sup> Regarding the transnational dimension of cybercrime, see *Keyser*, The Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, vol. 12, No. 2, page 289; *Sofaer/Goodman*, Cyber Crime and Security—The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq.

<sup>20</sup> For a brief history of the Internet, including its military origins, see *Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, Wolff*, “A Brief History of the Internet”, available at: <http://www.isoc.org/internet/history/brief.shtml>.

<sup>21</sup> Regarding the transnational dimension of cybercrime, see *Sofaer/Goodman*, Cyber Crime and Security—The Transnational Dimension, supra n. 19, page 7.

<sup>22</sup> Regarding the number of users of free-of-charge e-mail services see *Graham*, E-mail Carriers Deliver Gifts of Ninety Features to Lure, Keep Users, *USA Today*, 16.04.2008, The article mentions that the four biggest webmail providers have several hundred million users—Microsoft (256 million), Yahoo (254 million), Google (91 million) and AOL (48 million). Regarding the transnational dimension of Cybercrime, see *Keyser*, The Council of Europe Convention on Cybercrime, *Journal of Transnational Law & Policy*, vol. 12, No. 2, page 289; *Understanding Cybercrime: A Guide for Developing Countries*, ITU 2009, chapter 3.2.7.

<sup>23</sup> APWG Phishing Activity Trends Report, 1st Half 2009, page 7.

<sup>24</sup> Regarding the principle of National Sovereignty, see *Roth*, State Sovereignty, International Legality and Moral Disagreement, 2005, page 1, available at: <http://www.law.uga.edu/intl/roth.pdf>; *Martinez*, National Sovereignty and International Organizations, 1996; *Riegler*, Nation Building Between National Sovereignty and International Intervention, 2005.

<sup>25</sup> Regarding the need for international cooperation in the fight against Cybercrime, see *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, supra n. 19, page 35 et seq.

Timely and effective cooperation between competent authorities in different countries is crucial for the success of the investigation. There are two reasons for this: first, the speed of the transfer processes; and, second, the fact that evidence relevant for investigations is often automatically deleted within short time frames. Lengthy formal procedures can seriously hinder investigations.

A large number of existing mutual legal assistance agreements are still based on formal, complex and often time-consuming procedures.<sup>26</sup> The establishment of procedures which enable a quick response to incidents, as well as the timely submission of requests for international cooperation, is therefore vital.<sup>27</sup>

#### 4. Extent of organized crime involvement

As described further in detail below, the United Nations Convention against Transnational Organized Crime (UNTOC) is an important instrument for international cooperation. Its application is not limited to traditional crimes and can include identity-related offences if transnational organized crime is involved. As a matter of fact, the determination of the involvement of an organized criminal group—as required in Article 3(1) of the UNTOC—is highly relevant.

However, the analysis of the links between identity-related crime and organized crime presents difficulties. The first main obstacle is the absence of scientifically reliable research done in this area. Unlike the technical aspects of the offence—especially the scams used to obtain identity-related information<sup>28</sup>—the organized crime component of the offence is less intensively analyzed. Another obstacle is the lack of a universally accepted definition of identity theft<sup>29</sup> and related terminology.<sup>30</sup> This not only leads to difficulties in developing legislation, but could also negatively influence the research in this area.<sup>31</sup>

At the law enforcement level, successful investigations of identity-related crime cases reveal the involvement of organized criminal groups which meet the requirements of the definition of organized crime in Article 2(a) of the UNTOC. As a consequence, the involvement

<sup>26</sup> Gercke, Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, chapter 6.3.

<sup>27</sup> Gercke, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141.

<sup>28</sup> Regarding the methods used, see Gercke, Legal Approaches to Criminalize Identity Theft, Commission on Prevention and Criminal Justice, 18th session, 2009, E/CN.15/2009/CRP.13; Gercke, Understanding Cybercrime: A Guide for Developing Countries, supra n. 26, pages 59 et seq.

<sup>29</sup> Identity Crime, Final Report, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, 2008, page 7; Regarding definitions, see Finklea, Identity Theft: Trends and Issues, CRS, 2009, R40599, page 2; Paget, Identity Theft, McAfee White Paper, 2007, page 4.

<sup>30</sup> Finklea, Identity Theft: Trends and Issues, CRS, 2009, R40599, page 2. In the United Nations study on “fraud and the criminal misuse and falsification of identity”, released in 2007, the general term “identity-related crime” was used to cover all forms of illicit conduct involving identity, including identity theft and identity fraud. The reason was that Member States presently do not agree on definitions of these terms, and the same conduct designated as “identity theft” in some countries is seen as “identity fraud” in others. The term “identity theft”, in particular, was perceived to include cases in which information related to identity (basic identification information/other personal information) is actually taken in a manner analogous to theft or fraud, including theft of tangible documents and intangible information and deceptively persuading individuals to surrender documents or information voluntarily. On the other hand, the term “identity fraud” generally refers to the subsequent use of identification or identity information to commit other crimes or avoid detection and prosecution in some way. This includes both fraud against private entities (e.g. credit card fraud) and fraud against the public sector (e.g. illegally obtained social benefits or procurement contracts). See Results of the Second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, 02.04.2007, E/CN.15/2007/8/Add. 3, page 4.

<sup>31</sup> Results of the Second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, 02.04.2007, E/CN.15/2007/8, page 6.

of organized crime in this particular field is not questioned, but the determination of the extent of such involvement is still uncertain.

With regard to the definition of organized criminal group provided by Article 2(a) of UNTOC, two elements are of particular interest: the requirement of a group of three or more persons and a financial benefit. The third element, namely the nature of identity offences as “serious crimes”, will be mentioned below under chapter III, section 3.

#### *“A group of three or more persons”*

Committing an identity-related offence does not require the help of others,<sup>32</sup> as the necessary technology is available for offenders to carry out the offence alone. Nevertheless, investigations revealed the involvement of several crime gangs in identity-related crime cases. Most of those cases have in common that several offenders were involved in carrying out the offence. However, the structure of those groups is not necessarily comparable to that of traditional organized criminal groups. For example, cybercrime groups tend to have a looser and more flexible structure.<sup>33</sup> In addition, the size of the groups is often much smaller compared to traditional organized crime groups.<sup>34</sup> The Internet enables close cooperation with others and coordination of the activities without ever having met face-to-face.<sup>35</sup>

It is important to take into account that the term identity-related crime is not used to describe a single act crime, but a category of crime that very often combines different acts, including offences described, often not in a consistent manner, as “identity fraud” and “identity theft”. The fact that several offenders work together does not strictly mean that there is cooperation with others within each of the different phases of the criminal activity. A possible scenario demonstrating this feature is when, for example, one offender sends out “phishing” mails to obtain credit card information. The offender then hands over the whole set of data for a fixed price to a second offender that runs a website selling credit card data.<sup>36</sup> Finally, the credit card information is obtained by a third offender who uses the details to purchase goods.

Another possibility offered to offenders is to work together in non-stable ad hoc groups.<sup>37</sup> The question whether those groups meet the requirements of Article 2(a) and (c) of the UNTOC (definitions of “organized criminal group” and “structured group” respectively) should be further evaluated on a case-by-base basis. It should be noted, however, for purposes of further clarification and guidance on this matter, that an interpretative note to Article 2(c) of the UNTOC specifies that the term “structured group” is to be used in a broad sense so as to include both groups with hierarchical or other elaborate structure and non-hierarchical groups where the roles of the members of the group need not be formally defined”.<sup>38</sup>

<sup>32</sup> Report on Identity Theft, A Report to the Ministry of Public Safety Canada and the Attorney General of the United States, Bi-national Working Group on Cross-Border Mass Marketing Fraud, 2004; *Paget*, Identity Theft, McAfee White Paper, 2007, page 10.

<sup>33</sup> *Choo*, Trends in Organized Crime, 2008, page 273.

<sup>34</sup> *Brenner*, Organized Cybercrime, *North Carolina Journal of Law & Technology*, 2002, issue 4, page 27.

<sup>35</sup> See, for example, Convictions for Internet rape plan, Great Britain Crown Prosecution Service, Media release, 01.12.2006.

<sup>36</sup> Regarding the prices for credit card information, see Symantec Internet Security Threat Report, vol. XIII, 2008.

<sup>37</sup> *Choo*, Trends in Organized Crime, supra n. 34.

<sup>38</sup> See *Travaux Préparatoires* of the negotiations for the elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols thereto, United Nations, New York 2006, part one, page 17.

### *Financial benefit*

Whilst questions concerning the accuracy of statistics on the financial damage caused by identity theft offences remain open, it is certain that the losses as well as profits are significant. It is often the case that the financial losses of the victims directly correspond to the financial benefits of the offenders. One such example is found in cases where an offender purchases goods using the victim's credit card information. However, profit can be generated in prior steps as well—for example, by means of selling illegally obtained identity-related information. Prices depend on the category and quality of data and range from US\$10–1000 for bank account information<sup>39</sup> and US\$0.40–20 for credit card information.<sup>40</sup>

Apart from direct financial profit, offenders can use identity-related information to obtain indirect financial profit. In particular, they can use the victim's bank account to launder money. A significant number of measures to counter money-laundering are based on the “know-your-customer” principle and therefore, depend heavily on identity or identification elements. Money-laundering scams make use of information, communication and commercial technologies, which enable offenders to generate false identification information and further facilitate, through the use of such false identification, remote transfers aimed at concealing laundered assets.<sup>41</sup> In addition, they can circumvent identification and terrorist prevention measures by using obtained identities. The Report of the Secretary-General of the United Nations on recommendations for a global counter-terrorism strategy highlights the importance of developing tools to tackle identity theft in the fight against terrorism.<sup>42</sup>

Yet, within the debate about financial benefit, it is important to be aware that identity-related offences are not necessarily economic in nature or committed to gain direct or indirect financial profit. Perpetrators can use the information they obtain to hide their real identity<sup>43</sup> and thereby mislead investigations. However, such offences fall within the scope of the UNTOC when linked to an organized criminal group that is also involved in economic crime.

Moreover, the meaning of the term “financial or other material benefit” is relatively broad and includes for example, trafficking in child pornography for reasons of sexual gratification.<sup>44</sup> It therefore encompasses identity crimes where stolen or fabricated identification or identity information is treated as a form of illicit commodity and bought, sold or exchanged, as well as instances where identification is misused for personal or organizational gains, including non-financial gains such as securing entry into another country.

<sup>39</sup> Ibid.

<sup>40</sup> Ibid.

<sup>41</sup> Regarding the relation between identity-related offences and money laundering see: Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, Report of the Secretary-General, E/CN.15/2007/8/Add. 3, page 12.

<sup>42</sup> Uniting against Terrorism: Recommendations for a Global Counter-Terrorism Strategy, 27.04.2006, A/60/825, page 13.

<sup>43</sup> See, in this context, Results of the Second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity, supra n. 42, page 10.

<sup>44</sup> See *Travaux Préparatoires* of the negotiations for the elaboration of the United Nations Convention against Transnational Organized Crime and the Protocols thereto, supra n. 39, part one, page 17.

## II. GENERAL ASPECTS OF INTERNATIONAL COOPERATION IN IDENTITY-RELATED CRIME CASES

### 1. Importance of international cooperation in combating identity-related crime

In the past, crimes usually involved a national dimension and cross-border crime was an isolated phenomenon. Today, the emerging use of technology have enabled new forms of crime that led the academic world to speak about “the demise of territoriality”.<sup>45</sup> While criminals committing crimes do not seem to be limited by boundaries anymore, the criminal law rules still follow in most cases the traditional principle of national sovereignty, while very strict jurisdiction rules over a criminal offence are still in place. Thus, cooperation between States becomes essential.

Depending on the type of identity-related crime committed, investigation, prosecution and sentencing of the offender may presuppose an extraneous element. In cases of telephone fraud<sup>46</sup> or utilities fraud, for example, the offence occurs with predilection within a national territory of a determined state, while identity-related crimes committed through computer systems, such as “phishing” or “pharming”, frequently involve a multitude of victims situated in various states on different continents. The same applies to credit card fraud, which can have a regional component (implying countries located in a certain region), but also a global nature, especially if the credit card details were obtained or transferred through computer misuse.

As previously mentioned, a transnational element presupposes the necessity of international cooperation between States and, due to the nature of the offences, such cooperation has to be undertaken under certain conditions and, on many occasions, in a short period of time. This necessity of a fast response seems to jar with the traditional international cooperation, often characterized as “slow and cumbersome”.<sup>47</sup> The specificity of the international cooperation in these cases will be developed in the relevant chapters of the guide. Various types of requests could become applicable, but the most relevant ones are extradition (and its simplified version, applied within the EU, namely the European Arrest Warrant) and mutual legal assistance.

<sup>45</sup> See, for example, *Guinchard*, Criminal Law in the 21st century: the demise of territoriality? Notes for the Critical Legal Conference on Walls, 16 September 2007, Birkberk (London), available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1290049](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1290049).

<sup>46</sup> For details of types of telephone fraud, see: <http://www.ftc.gov/phonefraud>.

<sup>47</sup> See *Nielsen*, From classical judicial cooperation to mutual recognition, in *Revue Internationale de Droit Penal*, 77<sup>e</sup> année, nouvelle série, 1<sup>er</sup> et 2<sup>e</sup> trimestres 2006, page 53 et seq.

Given the nature of this guide, more emphasis will be placed on aspects of mutual legal assistance, as this form of international cooperation is part of the everyday work of judges and prosecutors dealing with identity-related crimes. This chapter merely provides an introduction into the main instruments which will be further developed in chapter III from a practical point of view, combined with a presentation of the main conventions applicable in identity-related crime cases. It will not only address the role of the judge or prosecutor who deals with international cooperation on a regular basis, but above all, the needs of the judge or prosecutor who has no previous experience in this respect and seeks general information about this subject matter.

## 2. Main instruments with reference to the international cooperation in combating identity-related crime

### *Extradition*

It is known that extradition has a long history, developing from the surrender of political offenders in ancient times,<sup>48</sup> to what is today, namely an institution allowing a State (the requested State) to provide assistance to another State (the requesting State) in surrendering an offender for the purposes of prosecution or enforcement of a sentence.

The extradition rules can be applied directly on the basis of a treaty which is self-executing according to the domestic laws of the requested State, or on the basis of a domestic law implementing the provisions of a treaty. Another possible scenario is that of extradition allowed on the basis of ad hoc arrangements concluded between two States when no other multilateral or bilateral treaty is in place. Usually, this kind of arrangement is based on the reciprocity requirement.<sup>49</sup> There are States granting extradition requests on the basis of reciprocity (e.g. Germany, Romania, Switzerland), while others are acting on the basis of an existing treaty only (e.g. the United States,<sup>50</sup> Belgium, United Kingdom and the Netherlands).<sup>51</sup>

All extradition treaties, whether international, regional or bilateral, comprise more or less the same principles, although the domestic laws reveal differences, bearing in mind the specificity of each legal system. The following chapter will briefly present the most

<sup>48</sup> It seems that the first treaty touching upon extradition was concluded between Ramses II of Egypt and the Hittite prince Hattushilish III. For details about the history of the extradition, see *Gilbert*, *Transnational Fugitive Offenders in International Law. Extradition and Other Mechanisms*, *Kluwer Law International*, 1998, page 17 et seq.

<sup>49</sup> The reciprocity rule entails that a State which requires the extradition of a person sought from the requested State obliges itself to consider the extradition request of that State under similar circumstances.

<sup>50</sup> As regards the United States, the United States Attorneys' Manual stipulates that in general, the extradition can be granted only pursuant to a treaty. Still, after the changes brought to the 18 USC 3181 and 3184 in 1996, it is allowed to grant extradition of persons (as long as they are not citizens, nationals or permanent residents of the United States) who have committed crimes of violence against nationals of the United States in foreign countries without making the existence of a treaty necessary. For details, see USAM Title 9-Chapter 9-15.000, available at: [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/15mcr.htm](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/15mcr.htm).

<sup>51</sup> See *Radu*, *Cooperare judiciară internațională și europeană în materie penală. Îndrumar pentru practicieni*, Wolters Kluwer, Romania, 2009, page 25.



significant elements to be taken into account with regard to the extradition of offenders committing identity-related crimes. It is important to acknowledge the nature of extradition as a procedure which entails the involvement of both the judicial and the executive branch. Whilst in some countries the role of the executive is more prevalent,<sup>52</sup> in others the judiciary holds the pre-eminence. Therefore, it is important for judicial authorities preparing documentation for extradition to bear in mind these general principles. The particularities of each treaty will be shortly discussed in the following pages.

### *Important elements related to the extradition procedure*

The conditions that need to be verified when formulating an extradition request refer to the offence itself, as well as to the offender. As this is not a guide dedicated to international cooperation per se, the following overview is limited to some of the most relevant features that need to be considered when formulating a request.

#### Seriousness of the offence

The extradition of a person is, in general, limited to offences of a certain gravity. This implies that such a complicated procedure requiring a significant mobilization of resources will not be used for minor offences. Some of the conventions establish different thresholds for prosecution than for the conviction or the execution of a detention order,<sup>53</sup> while others do not make such a distinction.

#### Double criminality requirement

The double criminality principle is one of the major requirements emerging from the legality principle.<sup>54</sup> Taking into account that identity-related offences are among those categories of crimes that are not yet globally criminalized, this principle is of specific importance with regard to identity-related crime. All extradition treaties<sup>55</sup> include the absence of double criminality as a mandatory ground of refusal.

Sometimes, especially in the case of bilateral instruments, the extradition can only be granted for a limited list of offences stipulated *expressis verbis* in the text of the specified treaty. While, for example, murder is an offence that is typically contained in such a list, identity-related crimes are typical examples of the so-called emerging crimes. With regard to such crimes, there is a risk that the requested State may not recognize them in its domestic law, or that the bilateral instrument may not include such offences among the

<sup>52</sup> There are different national approaches regarding the decision-making in extradition process. For example, in the United States the final decision is taken by the Secretary of State, while in Romania the decision to extradite a person is taken by a judicial authority.

<sup>53</sup> See, for example, the European Convention on Extradition, Paris 1957, available at: <http://conventions.coe.int/Treaty/EN/Treaties/Html/024.htm>.

<sup>54</sup> Dual criminality exists if the offence is a crime under the laws of both the requested and requesting parties. Regarding the dual criminality principle in international investigations, see *United Nations Manual on the Prevention and Control of Computer-Related Crime, International Review of Criminal Policy*, Nos. 43 and 44: United Nations publication, Sales No. E.94.IV.5, page 269; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, presented at the ITU Thematic Meeting on Cybersecurity held in Geneva from 28 June to 1 July 2005, page 5.

<sup>55</sup> See, for example, Article 2 of the European Convention on Extradition, Paris, 1957, Article 3 of the Inter-American Convention on Extradition, Caracas, 1981, etc.

listed ones, especially if the bilateral treaty was concluded in the past<sup>56</sup> at a time when identity-related crime was not recognized as an illegal act and no amendments or updates of the list of offences were agreed upon.

It should be noted that in general the modern extradition treaties, whether bilateral or multilateral, have renounced this “list” criterion,<sup>57</sup> opting in for the “punishability” criterion, which is more effective, due to its flexibility.

Taking into account different approaches to criminalize identity-related crimes,<sup>58</sup> another situation, which could be encountered in the context of international cooperation, is where identity theft is not included as a specific offence, but some of its different phases (preparatory acts, obtaining the information, transfer process, use for criminal purposes)<sup>59</sup> are covered. Therefore it is important for the competent authorities of the requesting State to provide precise information on the offences for which extradition is sought and the relevant provisions of its legislation establishing such offences.

The often transnational nature of the crime of identity-related crime, which brings challenges to the very notion of territoriality, can underscore problems with regard to the interpretation of the double criminality rule if the requesting and requested States are based on different legal traditions.<sup>60</sup>

Recent trends and developments in extradition law have focused on relaxing the strict application of certain grounds for refusal of extradition requests. In this context, attempts have been made to ease the difficulties with double criminality as well, by inserting general provisions into treaties which simply allow extradition for any conduct criminalized and subject to a certain level of punishment in both the requested and requesting States. In view of that, steps should be taken at the regional level towards harmonization of national legislations, to the greatest extent possible, in particular in connection with the provisions on criminalization set out in the United Nations Convention on Transnational Organized Crime and its Protocols, as well as the United Nations Convention against Corruption, so that the principle of dual criminality would not constitute an obstacle to developing more effective cooperative arrangements.<sup>61</sup>

---

<sup>56</sup> Such an example was represented by an old bilateral treaty applicable between the United States and the United Kingdom according to which the extradition from the United Kingdom to the United States depended upon the fact that the offence should have been part of the listed offences. In the United Kingdom this list was enshrined by the Extradition Act 1870 which did not, of course, cover the wire fraud offences stipulated by the United States criminal law. There was no equivalent offence in the British law, apart from a similar concept—conspiracy to defraud, which was not among the 1870 offences list also. This was quite an inconvenient situation, which was surpassed by means of a new treaty which, instead of the list system, introduced the one based on punishability, see *Joshi/Gibbins*, Reform of the United Kingdom Extradition Law in United States Attorneys’ Bulletin, September 2003, page 51 et seq., available at: [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usab5105.pdf](http://www.justice.gov/usao/eousa/foia_reading_room/usab5105.pdf).

<sup>57</sup> The list criterion is considered by literature as presenting some drawbacks compared with the tendency imposed by the modern treaties to make reference to a minimum level of punishment. For details, see *Bantekas/Nash*, International Criminal Law, Routledge-Cavendish, 2007, page 296.

<sup>58</sup> Regarding the different approaches, see *Gercke*, Legal Approaches to Criminalize Identity Theft, supra n. 28.

<sup>59</sup> *Ibid*, pages 38 et seq.

<sup>60</sup> In those cases there are differences of interpretation in civil law countries in comparison to common law countries, in the sense that in general, the civil law countries prosecute irrespective of the fact that the alleged crime took place partially or totally outside their territory, see *Bantekas/Nash*, International criminal law, supra n. 57, page 297.

<sup>61</sup> It should be noted that Article 43(2) of the United Nations Convention against Corruption (UNCAC) requires that, whenever double criminality is necessary for international cooperation, States Parties must deem this requirement fulfilled, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States parties, regardless of the legal term used to describe the offence or the category within which such offence is placed.

## Ne bis in idem

This traditional principle, founded on both humanitarian considerations and the need for ensuring the proper administration of justice, requires that a person cannot be extradited if he/she has already been sentenced in the requested State for the same offence for which the extradition is being requested.<sup>62</sup> This is an example of a mandatory ground for refusal,<sup>63</sup> whereas if extradition is requested for prosecution purposes, ne bis in idem is rather an optional ground for refusal.<sup>64</sup>

## *Aut dedere aut judicare* ("extradite or prosecute")

This principle ensures that if one State does not extradite the person sought, it has to take over the criminal procedure against that person upon request of the requesting State. It is intended to prevent the creation of safe havens for criminals. Any modern extradition treaty<sup>65</sup> or international instrument including provisions on extradition<sup>66</sup> recognizes this principle.

## Lapse of time

This is another condition which provides protection from extradition if the person sought cannot be prosecuted or punished because of lapse of time. Some more recent extradition treaties have renounced the condition of verifying whether the statutory limitation is applicable in the requested State, considering that such a request causes difficulties in the cooperation between the requesting and the requested States.

## Speciality rule

Under the speciality rule, a person once extradited cannot be proceeded against, sentenced or detained for offences committed prior to his/her surrender, other than those which led to the extradition request. Of course, there are some limited exceptions to this rule, such as in case the requested State consents to the extension of the extradition request. This situation represents a realistic scenario in cases of identity-related crimes, where offences not known at the time of submission of the extradition request are detected after such submission.

<sup>62</sup> For details, see *Vervaele*, The transnational ne bis in idem. Principle in the European Union: Mutual Recognition and Equivalent Protection of Human Rights, *Utrecht Law Review*, vol. 1, No. 2, pages 100-118; *Conway*, ne bis in idem in International Law, *International Criminal Law Review*, vol. 3, No. 3, pages 217-244; 2003, the Explanatory Report to the European Convention on the Transfer of Proceedings in Criminal Matters, available at: <http://conventions.coe.int/Treaty/en/Reports/Html/073.htm>.

<sup>63</sup> See Article 9, first sentence of the European Convention on Extradition, Paris 1957 or Article 4(d) of the Protocol on Extradition of the Southern African Development Community, 2002.

<sup>64</sup> See Article 9, second sentence of the European Convention on Extradition, *ibid*, or Article 5(i) of the Protocol on Extradition of the Southern African Development Community, *ibid*.

<sup>65</sup> See, for example, Article 8 of the Inter-American Convention on Extradition, available at: [www.oas.org/juridico/english/treaties/b-47.html](http://www.oas.org/juridico/english/treaties/b-47.html), which states that: "If, when extradition is applicable, a State does not deliver the person sought, the requested State shall, when its laws or other treaties so permit, be obligated to prosecute him for the offence with which he is charged, just as if it had been committed within its territory, and shall inform the requesting State of the judgement handed down—the article refers to the hypothesis of taking over the prosecution".

<sup>66</sup> See Article 16(12), the United Nations Convention against Transnational Organized Crime, Palermo, 2000 (hereinafter UNTOC): "If extradition, sought for purposes of enforcing a sentence, is refused because the person sought is a national of the requested State Party, the requested Party shall, if its domestic law so permits and in conformity with the requirements of such law, upon application of the requesting Party, consider the enforcement of the sentence that has been imposed under the domestic law of the requesting Party or the remainder thereof".

## Other principles

One of the traditional principles guiding the extradition procedure is that of the “non-extradition of nationals”.<sup>67</sup> This principle mostly emerges in civil law systems, while this is not the case in common law jurisdictions. However, even in civil law systems there may be cases where extradition of nationals is permitted under some strict conditions.<sup>68</sup>

The reluctance to extradite their own nationals appears to be lessening in many States. The UNTOC includes a provision reflecting this development: Article 16(11) refers to the possibility of a temporary surrender of the fugitive on condition that he or she will be returned to the requested State party for the purpose of serving the sentence imposed. In cases where the requested State refuses to extradite a fugitive on the grounds that the fugitive is its own national, the State has often the obligation to bring the person to trial. This is an illustration of the principle of *aut dedere aut judicare* (“extradite or prosecute”), which was briefly presented above. Where extradition is requested for the purpose of enforcing a sentence, the requested State may also enforce the sentence that has been imposed in accordance with the requirements of its own domestic law.

In addition, grounds for refusal of an extradition can be founded on human rights considerations, such as the death penalty or discrimination based on race, religion, nationality, ethnic origin or political opinion.<sup>69</sup> In general, the traditional<sup>70</sup> extradition treaties include provisions which forbid the extradition for political or military offences.

Another important principle that needs to be briefly mentioned is that of the rule of non-inquiry. In broad terms, the rule of non-inquiry stipulates that the judicial authorities of the requested State should not inquire into the good faith or the motive of an extradition request.<sup>71</sup>

## Practical and formal requirements

Extradition is a rather formal procedure. There are several practical aspects which must be taken into account, when referring to the documents accompanying the extradition request. This consideration may slightly differ depending on the legal systems of the States

<sup>67</sup> This principle has its roots in the sovereignty rule as well, being enshrined on many occasions even in the fundamental laws. The application of this principle depends on the interpretation offered by each domestic law with regard to the term “national”. See, for example, the case of the Nordic States which assimilate to nationals all the registered residents—see *Bantekas/Nash*, *International Criminal Law*, supra n. 57, page 308.

<sup>68</sup> See, for example, Article 26(1) of the Italian Constitution which stipulates that the extradition of a citizen is permitted only in cases expressly provided for in international conventions.

<sup>69</sup> The political offence doctrine mainly states that the extradition shall be refused if it was solicited for some crimes connected with the political order in the requesting country. For more details in this regard and the historical evolution, see *Cervasion*, *Extradition and the International Criminal Court: The Future of the Political Offence Doctrine*, Issue No. *Pace International Law Review*, vol. No., 1999, pages 419 et seq. Though this rule has less practical importance from the perspective of identity-related crime.

<sup>70</sup> See the European Convention on Extradition, Paris 1957, which still applies for those member States of the Council of Europe which are not member States of the European Union or for member States of the European Union which have deposited declarations to the Framework Decision on the European Arrest Warrant and the surrender procedure of the member States, stating that they continue to apply the extradition procedure under some strict conditions (see the statements rendered by Italy, Austria, France, Czech Republic, Luxembourg). For details see the *European Handbook on How to Issue a European Arrest Warrant* in *Instruments on Judicial Cooperation in Criminal Matters within the Third Pillar of the European Union and Other Essential International Instruments on Judicial Cooperation*, Consilium, 2009, page 493 or available online at: [www.gddc.pt/MDE/Manual\\_MDE\\_EN.pdf](http://www.gddc.pt/MDE/Manual_MDE_EN.pdf).

<sup>71</sup> For details, see *Bantekas/Nash*, supra n. 57, page 309. Regarding a possible partial exception in those cases when extradition is sought for judgments rendered in absentia, see *Pyle*, *Extradition, Politics and Human Rights*, Temple University Press, 2001, page 127.

involved, but there are some common elements not related to any specific legal system. Information which needs to be provided to the competent authorities of the requested State includes, for example, the following: particulars of the person sought, arrest warrant or criminal judgment issued against the extraditable person, summary of the facts and applicable legal provisions. The related documents need to be certified. The certification requirements may differ from one country to another, but in general the certification is a task of the judicial authority preparing the documentation. Common law countries have certain particularities,<sup>72</sup> especially in respect of the annexed documents which need to be presented in a certain form<sup>73</sup> in order to be admissible in the court. When formulating a request, it is important that the requesting State is aware of the special formal requirements. Some States accept the transmittal of the requests and the annexed documents directly from a central authority to a central authority, but most of them still make use of their diplomatic channels.

It is common knowledge that different prosecutorial practices under both common law and continental law systems make effective interregional and international cooperation more difficult. In the field of extradition, these differences are even more acute when dealing with the documents required to be presented to the requested State and the relevant evidentiary requirements needed for granting an extradition request.

In most continental law States, extradition is viewed as a tool of international cooperation for bringing a fugitive offender to justice. The objective of the extradition mechanism is to surrender the person sought to proceedings conducted abroad. According to this concept, courts dealing with extradition cases abstain from examining the evidence of guilt against the person sought, as they consider that this examination is incumbent exclusively upon the judicial authorities of the requesting State. The authorities of the requested State content themselves with the fact that a valid judicial warrant of arrest based on an extraditable offence exists, that the substantive and procedural requirements for extradition are met, and that none of the contractually or statutorily stipulated grounds for refusal of an extradition request apply in the given case.

In contrast, in many common law States, it is required that the initiation of the extradition process complies with the general standards for the initiation of a criminal procedure. Consequently, the inquiry goes further than a formal control of extradition conditions and the competent judicial authority examines whether the request contains reasonable grounds to believe, or probable cause to believe, that the person wanted has committed the crime charged with or whether the request provides “prima facie evidence of guilt” that would be sufficient to justify the committal of the accused person for trial in the requested State.<sup>74</sup> In view of the fact that the “prima facie evidence of guilt” has proved in practice to be an outstanding impediment to extradition not only between systems of different legal tradition but also between countries with the same general traditions but differing rules of

<sup>72</sup> In common law countries the prima facie evidence is among the requirements that need to be fulfilled. This is so, for example, in the case of Canada. See: <http://laws.justice.gc.ca/eng/E-23.01/20100304/page-2.html?rp2=HOME&rp3=SI&rp1=extradition&rp4=all&rp9=cs&rp10=L&rp13=50>, or even Israel at: [http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/transnational\\_criminal\\_justice/2\\_pc-oc/israel's%20prima%20facie%20evidence%20requirements.pdf](http://www.coe.int/t/e/legal_affairs/legal_co-operation/transnational_criminal_justice/2_pc-oc/israel's%20prima%20facie%20evidence%20requirements.pdf).

<sup>73</sup> For example, Canada has very specific requirements as regards the form of the extradition request, which has to be presented in front of their authorities, depending on the fact that the decision was rendered in absentia or not.

<sup>74</sup> See, inter alia, the Revised Manual on the Model Treaty on Extradition, Commission on Crime Prevention and Criminal Justice, thirteenth session (Vienna, 11-20 May 2004), E/CN.15/2004/CRP.11, pages 32-33, paragraph 108.

evidence, and given that several common law States have waived this requirement in prescribed circumstances, it is recommended that States keep the burden of proof in extradition proceedings to a minimum and take into account in their extradition relations the need for simplification of the evidentiary requirements (see also Article 16(8) of the UNTOC and Article 44(9) of the UNCAC).

### *European Arrest Warrant*

Although this mechanism is used only within the European Union, it is important to be noted as a tool for international cooperation<sup>75</sup> because the caseload developed among the European Union up to this moment underlines the efficiency of this tool with regard to credit card fraud cases and “phishing” schemes.<sup>76</sup> This kind of cooperation has been introduced by the Framework Decision 2002/584/JHA of 13 June 2002 (FD) on the European arrest warrant and the surrender procedure between the member States<sup>77</sup> in line with the main criminal policies brought at the European Union level by the European Council under the Tampere Programme.<sup>78</sup> The process of the European arrest warrant has been highly rated by some and criticized by others, raised constitutional problems in some member States,<sup>79</sup> and is being continuously evaluated.<sup>80</sup>

The EAW process introduces the following novelties compared to the former extradition procedures:

*Expeditious proceedings:* The final decision on the execution of the EAW should be taken within a maximum period of 90 days after the arrest of the requested person. If that person consents to the surrender, the decision shall be taken within 10 days after consent has been given (Article 17).

*Abolition of double criminality requirement in prescribed cases:* The deeply ingrained in traditional extradition law double criminality principle shall not be verified for a list of 32 offences, which, according to Article 2(2) of the Framework Decision, should be punishable in the issuing Member State for a maximum period of at least 3 years of imprisonment and defined by the law of this Member State. These offences include, inter alia, participation in a criminal organization, terrorism, trafficking in human

<sup>75</sup> For a detailed presentation of the instrument, see *Kreijzer/Van Sliedregt*, *The European Arrest Warrant in Practice*, T.M.C Asser Press, 2009.

<sup>76</sup> See, for example, the EUROJUST Report 2008 and the EUROJUST Report 2007 where joint actions as regards the execution of EAW issued for phishing and skimming were mentioned, available at: <http://www.eurojust.europa.eu/>.

<sup>77</sup> Published in the *Official Journal* L 190, 18/07/2002 pages 1-20.

<sup>78</sup> It is common knowledge that the consensus of the Member States and the idea that stood behind this FD resided in the 9/11 terrorist attacks which determined a clear and rapid response from the European Union by creating an instrument which would have facilitated the fight against terrorism and serious crimes.

<sup>79</sup> Germany, Poland and Cyprus were three of the Member States where the Constitutional Courts released decisions against the constitutionality of domestic laws transposing the Framework Decision. For details see the European Handbook on How to Issue a European Arrest Warrant in Instruments on Judicial Cooperation in Criminal Matters within the Third Pillar of the European Union and other Essential International Instruments on Judicial Cooperation, Consilium July 2009, page 490 et seq. The first two decisions are available in English as follows: the judgment of 27 April 2005 of the Polish Constitutional Tribunal, P 1/05, at: [http://www.trybunal.gov.pl/eng/summaries/summaries\\_assets/documents/P\\_1\\_05\\_full\\_GB.pdf](http://www.trybunal.gov.pl/eng/summaries/summaries_assets/documents/P_1_05_full_GB.pdf), the judgment of 18 July 2005, 2 BvR 2236/04 of the German Federal Constitutional Court, at: [http://www.bundesverfassungsgericht.de/en/decisions/rs20050718\\_2bvr223604en.html](http://www.bundesverfassungsgericht.de/en/decisions/rs20050718_2bvr223604en.html).

<sup>80</sup> Several evaluation rounds took place since the European Arrest Warrant has been introduced in the legal systems of the EU member States: the most recent evaluations undertaken in the framework of the Fourth Round of Mutual Evaluation were conducted in the late 2008 and referred to Bulgaria and Romania.

beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in weapons, munitions and explosives, corruption, fraud including that affecting the financial interests of the European Communities, laundering of the proceeds of crime, computer-related crime, environmental crime, facilitation of unauthorized entry and residence, murder and grievous bodily injury, rape, racism and xenophobia, trafficking in stolen vehicles, counterfeiting currency etc. For offences which are not included in the abovementioned list or do not fall within the three years threshold, the double criminality principle still applies (Article 2(4)).

*“Judicialization” of the surrender:* The new surrender procedure based on the EAW is removed outside the realm of the executive and has been placed in the hands of the judiciary. Both the issuing and executing authorities are considered to be the judicial authorities which are competent to issue or execute a EAW by virtue of the law of the issuing or executing Member State (Article 6). Consequently, since the procedure for executing a EAW is primarily judicial, the administrative stage inherent in extradition proceedings, i.e. the competence of the executive authority to render the final decision on the surrender of the person sought to the requesting State, is abolished.

*Surrender of nationals:* The European Union Member States can no longer refuse to surrender their own nationals. The Framework Decision does not include nationality as either a mandatory or optional ground for non-execution. Furthermore, Article 5(3) provides for the option of making execution conditional on a guarantee that, upon conviction, the individual is returned to his/her State of nationality to serve the sentence there.

*Abolition of the political offence exception:* The political offence exception is not enumerated as mandatory or optional ground for non-execution of a EAW. The sole remaining element of this exception is confined to the recitals in the preamble of the Framework Decision (recital 12) and takes the form of a modernized version of a non-discrimination clause.

*Additional deviation from the rule of speciality:* Article 27(1) of the Framework Decision enables Member States to notify the General Secretariat of the Council that, in their relations with other Member States that have given the same notification, consent is presumed to have been given for the prosecution, sentencing or detention with a view to carrying out of a custodial sentence or detention order for an offence committed prior to surrender, other than that for which the person concerned was surrendered.

### Channels and means of communication

This is another important element that differentiates the EAW from the traditional extradition system in the sense that it promotes direct contact between the judicial authorities, whether requesting or requested, eliminating intermediary links such as diplomatic channels or central authorities. The central authorities remain in operation when the legal system allows it, being responsible for the administrative transmission and reception of the

European arrest warrant<sup>81</sup>. The framework decision allows the use of fax or e-mail in transmitting the EAW.<sup>82</sup> The direct contact and the use of expedited means of communication are a significant advantage in the fight against identity-related crime, which needs to be dealt with in timely manner.

### *The CARICOM Arrest Warrant*

Another regional instrument which is similar to the EAW is the CARICOM Arrest Warrant, established by the states from the Caribbean Region through the CARICOM Arrest Warrant Treaty.<sup>83</sup> It was adopted in 2008 and promotes a simplified extradition procedure by facilitating the contact of the judicial authorities from the requesting and requested state.<sup>84</sup>

According to the definition stipulated in Article I, “CARICOM arrest warrant means an arrest warrant issued by the issuing judicial authority of one State Party [...] with a view to the arrest and surrender of a requested person by the executing judicial authority of another State Party for the purposes of conducting a criminal prosecution or executing a custodial sentence”. Like the EAW, the instrument mentions urgency<sup>85</sup> and also uses the term “surrender”.

The transmittal and reception of the CARICOM arrest warrant is made through central authorities, but the decision to issue such an arrest warrant or to execute it belongs to the judicial authorities: the instrument allows the use of expedited means of communication.<sup>86</sup>

### *Mutual legal assistance and particularities emerging from the identity-related crimes*

Mutual legal assistance (MLA) requests are essential in solving cases having a transnational character. Identity-related offences are impossible to be addressed effectively without the prompt and efficient cooperation of police and judicial authorities worldwide. While regional approaches prove to be sufficient in typical MLA cases, this does not apply entirely when dealing with identity-related crime. A typical MLA request involves a requesting State and a requested State. Conversely, when referring to identity-related crime, for example, this is not entirely accurate. On many occasions, there is a need to transmit requests to more than one countries, there are even situations when the requests are directed towards three continents, particularly in cases of computer-related fraud and forgery. This is an exemplification of the transnational character of identity-related crime.

<sup>81</sup> There are Member States such as Italy, United Kingdom and Ireland, that make use of this provision in all cases so that the EAWs are received or transmitted only through the Ministries of Justice.

<sup>82</sup> Article 10(4) of the Framework Decision states that “the issuing judicial authority may forward the European arrest warrant by any secure means capable of producing written records under conditions allowing the executing Member State to establish its authenticity”. There are Member States that condition the surrender of the offender to the submital of the original documents emanating from the requesting judicial authority.

<sup>83</sup> CARICOM is the abbreviation for the Caribbean Community, for a list of the member states and associate members, see: <http://www.caricomlaw.org>.

<sup>84</sup> The text of the Treaty is available at: [www.caricom.org/jsp/secretariat/legal\\_instruments/caricom\\_arrest\\_warrant\\_treaty.pdf](http://www.caricom.org/jsp/secretariat/legal_instruments/caricom_arrest_warrant_treaty.pdf).

<sup>85</sup> See Article X of the Treaty: In case the person consents to the surrender, the decision of the judicial authority has to take place within 48 hours after the consent has been given.

<sup>86</sup> See Article VII of the Treaty.



Most of the MLA requests are issued during the pre-trial phase, taking into account that the prosecution is, on many occasions, based on evidence or information gathered from abroad. There are also requests formulated during the trial proceedings, such as summons of injured parties, hearing of victims or requests of information as criminal records of potential offenders.

Before discussing the challenges posed by the transnational nature of identity-related crime, it should be highlighted that, in general, the principles presented under the extradition section remain, to a certain degree, valid and applicable with regard to mutual legal assistance as well (e.g. double criminality, *ne bis in idem*, human rights considerations, and reciprocity in the absence of an applicable treaty).

There are several types of MLA requests that can be issued: a letter rogatory (with various subjects of request), taking evidence or statements from suspects, victims and witnesses, sometimes by using videoconference, effecting service of judicial documents, executing freezing or confiscation of assets. Joint investigation teams or the 24/7 networks of point of contacts established for cybercrime offences are also relevant when discussing MLA requests in identity-related crime cases with a transnational character.

In addition, there are new forms of mutual assistance which are extremely useful for this type of crime. These new forms of MLA, brought by the Council of Europe Cybercrime Convention, are now more frequently used in identity-related crime cases. They aim at ensuring rapid responses from the requested States, through expedited preservation of stored computer data, mutual assistance regarding accessing of stored computer data, mutual legal assistance in real time collection of traffic data or mutual assistance regarding the interception of content data (for details, see Articles 29 to 34 of the Council of Europe Cybercrime Convention, which will be presented in relevant parts of the guide).

What follows is a brief overview of challenges encountered in MLA cases involving identity-related crimes.

### Multitude of legal instruments applicable

While formulating a single request, there might be more than one international legal instrument that needs to be taken into consideration. Therefore, the judicial authority formulating the request needs to know if one of the legal instruments has pre-eminence with regard to one State, or in case there are several requested States, which convention is applicable to each of them. It is essential to invoke the right legal instrument, as many states still have very strict formal requirements and requesting their assistance on the basis of a non-applicable treaty can cause their refusal to execute the request. One of following subchapters provides an overview about those regional and international treaties that are or could be used with regard to identity-related crime. It is necessary to point out that while some treaties have opted in for modern ways of communication that allow a speedier communication, others still require the cooperating States to use diplomatic channels for the transmission of requests.<sup>87</sup>

<sup>87</sup> The Korean legislation in the field, for example, establishes a rule for traditional MLA, demanding a request to be transmitted or received through diplomatic channels only. Though, in urgent cases fax and e-mails are allowed, for details see *Knoops/Brenner*, *Cybercrime and Jurisdiction*, A Global Survey, Asser Press 2006, page 271.

## Volatility of data

As mentioned in the introductory part, this guide places put emphasis on cases of identity-related crime, committed either in an online environment or by means of computer-enabled technology, as these cases are most likely to have a transnational dimension. While transfer processes using network technology can be completed within seconds, provision of the mutual legal assistance is slow whenever “conventional” channels or means of communication are used. Sometimes a rapid response to requests related to the use IP addresses or submission of log files are of great importance for the continuation of the investigation. However, the response rate and the accuracy of the response are dependent upon the time necessary to forward the MLA request to the executing authority.<sup>88</sup> In skimming cases, the videotape from an ATM machine situated in another country cannot be saved if the request is not made and executed in a timely manner, as, in many countries, banks preserve the video files for short periods of time only. These kind of requests need to be dealt with urgency, using the expedited means of communication such as fax or e-mail.

## Double criminality requirement

As already mentioned, double criminality is one of the major principles of international cooperation. It derives from the sovereignty and legality principles and—depending upon the legal instrument in force—is applicable with regard to mutual assistance requests as well.<sup>89</sup> Recalling its details, it should be highlighted that a convergence of legal substantive provisions with regard to identity-related crime could assist in overcoming impediments or difficulties posed by such a requirement.

However, in view of the fact that many of the existing grounds for refusal of a mutual legal assistance request in bilateral, regional or multilateral instruments are a “carry-over” from extradition treaties, legislation and practice, where life or liberty of the requested person is more directly and immediately at stake,<sup>90</sup> States could consider whether it is necessary to retain such grounds for refusal or to minimize them and exercise them sparingly. Consideration should also include whether States desire to retain or exclude the double criminality requirement in mutual legal assistance schemes as a whole.

One possible way to overcome problems posed by the requirement of “identical legal labels” is to ensure that, in determining the application of the double criminality requirement, the underlying conduct of the offence will be taken into account regardless of the denomination or categorization of the offence under the laws of both requested and requesting States.<sup>91</sup>

<sup>88</sup> For some practical examples on the slowness of the classical mutual assistance and the impediments caused by such a slow process, see *Elston/Stein*, *International Cooperation in On-line Identity Theft Investigations: A Hopeful Future but a Frustrating Present*, available at: <http://www.isrc.org/Papers/Elston%20and%20Stein.pdf>.

<sup>89</sup> See Article 18(9) UNTOC, which stipulates that: “states parties may decline to render mutual legal assistance pursuant to this article on the ground of absence of dual criminality”.

<sup>90</sup> See the Report of the UNODC Expert Working Group on Mutual Legal Assistance Casework Best Practice (Vienna, 3-7 December 2001), page 11. The Report is available at: [http://www.unodc.org/pdf/lap\\_mlaeg\\_report\\_final.pdf](http://www.unodc.org/pdf/lap_mlaeg_report_final.pdf).

<sup>91</sup> See, in particular, Article 43(2) of the United Nations Convention against Corruption.

## Positive conflicts of jurisdiction

The problem of jurisdiction<sup>92</sup> is one of the main issues raised within the debate about transnational crime. As practitioners underline, when dealing with cybercrime and identity-related crime, it is often difficult to determine where the offence has been committed and which State is entitled to defer the criminals to justice. The claims for jurisdiction raised by several States lead to positive conflicts of jurisdiction. This happens frequently with regard to computer-related fraud, forgery or credit card cloning, as both States, where the victims and the offender are located, conduct parallel investigations.

Which of the countries involved is more entitled to have priority and to what extent extra-territorial jurisdiction can be applied in Internet-related cases are questions that have caused much controversy in specialized literature.<sup>93</sup> Provisions referring to the spontaneous exchange of information or to the *aut dedere aut judicare* principle can partially improve a general situation. In the absence of a legal framework adapted to this context, constant cooperation and contacts in real time among law enforcement are key factors in preventing the occurrence of these conflicts of jurisdiction.

## Execution of MLA requests in a foreign State

One of the major difficulties in providing mutual legal assistance relates to the execution of the request in a form admissible in the legal system of the requesting state. In view of existing differences between the legal systems of Member States, the requested State may have specific requirements, e.g. for obtaining a judicial order or taking evidence from persons, unknown to the requesting state, thus creating delays, wastage and frustration. It is, therefore, important that the legal frameworks of Member States are flexible and adaptable enough, to assist a variety of countries and several different legal systems. For example, Article 18(17) of the UNTOC provides that a mutual legal assistance request shall be executed in accordance with the domestic law of the requested State party and, to the extent not contrary to this law and where possible, in accordance with the procedures specified in the request. In parallel, the Model Treaty on Mutual Assistance in Criminal Matters<sup>94</sup> enables the execution of the request in the manner specified by the requesting State “to the extent consistent with the law and practice of the requested State” (Article 6).<sup>95</sup>

To overcome the above-mentioned difficulties, Member States could consider alternatives such as the practice of locating liaison persons<sup>96</sup> at the central authorities of countries in

<sup>92</sup> The problem of jurisdiction on the Internet is extensively discussed in *Koops/Brenner*, *Cybercrime and Jurisdiction*, A Global Survey, Asser Press 2006; *Kohl*, *Jurisdiction and the Internet*, A Regulatory Competence over Online Activity, Cambridge University Press, 2007 or *Kaspersen*, *Cybercrime and Internet Jurisdiction*, A Discussion Paper, prepared under the Council of Europe Project on Cybercrime, 5 March 2009, available at: [http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20\(2009\)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf](http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2009)%20draft%20discussion%20paper%20Cybercrime%20and%20jurisdiction.pdf).

<sup>93</sup> See, for example, *Koops*, *Cybercrime Jurisdiction: Introduction*, in *Koops/Brenner*, *Cybercrime and Jurisdiction*, supra n. 87, page 6; *Brenner*, *The Next Step: Prioritizing Jurisdiction*, *ibid*, page 327 et seq.; *Goldsmith*, *The Internet and the Legitimacy of Remote-Cross-border Searches*, 1 *University of Chicago Legal Forum* 103 (2001), available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=285732](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732); *Seitz*, *Transborder Search, A New Perspective?*, 7 *Yale Journal of Law and Technology* 23, 2004-2005.

<sup>94</sup> Adopted by the General Assembly Resolution 45/117 of 14 December 1990 and subsequently amended by the General Assembly resolution 53/112 of 9 December 1998.

<sup>95</sup> See the Revised Manual on the Model Treaty on Mutual Assistance in Criminal Matters, Commission on Crime Prevention and Criminal Justice, thirteenth session (Vienna, 11-20 May 2004), E/CN.15/2004/CRP.11, page 96 et seq.

<sup>96</sup> A separate subchapter of the guide will make reference to the institution of the liaison magistrate.

the region or of key countries of a region or continent, with which there is enough volume or value of cooperation casework to justify their placement. Such an initiative could prove to be very effective and successful, particularly in complex and urgent cases, given that liaison officials assist in accommodating the way requests are both made and executed. They could also substantially reduce the amount of waste papers and delays unavoidable in the traditional back and forth movement of documents, as often, the incoming requests do not comply with the laws or procedures of the requested State.<sup>97</sup> The use of regional networks could also be of significant assistance in achieving this task.

### Informal cooperation<sup>98</sup>

Online identity-related crimes often take place in a very short period of time and investigations need to be fast to ensure that relevant information is not destroyed in the meantime. Particularly in light of this, the traditional MLA tools need to be accordingly adapted in order to be efficient and effective. Sometimes the piece of information gathered by means of informal cooperation can be used to collect information necessary to speed up the formal process. Therefore, the police cooperation undertaken in the framework of institutions such as Interpol or Europol is of great relevance. Such information can, for example, be used for the further collection of initial identification data of potential offenders, a preliminary issue in the investigation and prosecution of identity-related crime. Still, this kind of inter-police or inter-law enforcement cooperation will not refer to gathering of evidence for court proceedings, as long as such an activity generally requires a formal request. In general, informal cooperation is intrinsically linked to publicly available data. Usually, international, regional and bilateral instruments contain provisions dealing with this type of cooperation under corresponding titles, such as “Law Enforcement Cooperation”.<sup>99</sup> Other methods of informal cooperation include exchange of memoranda of understanding and mutual administrative arrangements.<sup>100</sup>

### *Joint investigation teams*

Another important form of international cooperation is the establishment of joint investigation teams. The idea behind this modality of cooperation is to facilitate mutual legal assistance in transnational cases where the subject of investigations, prosecutions or judicial proceedings involves more than one State. Therefore offences such as drug trafficking, trafficking in human beings and identity-related crime, which are transnational by nature, can be dealt with through resort to joint investigation teams also.

Sometimes domestic laws of many countries permit collaborative and cooperative approaches and joint investigative practices. However, the experience suggests that legal as well as other difficulties remain in establishing effective joint investigations.

<sup>97</sup> See the Report of the Informal Expert Working Group on Effective Extradition Casework Practice, Vienna, 2004, page 14, available at: <http://www.unodc.org/unodc/en/legal-tools/training-tools-and-guidelines.html>.

<sup>98</sup> Advantages of having in place informal cooperation and conditions under which such cooperation can take place can be found in the Report of the Informal Expert Working Group on Mutual Legal Assistance Casework Best Practice, Vienna 2001, page 9, supra n. 90.

<sup>99</sup> See, for example, Article 27 of the UNTOC.

<sup>100</sup> See *Bantekas/Nash*, International Criminal Law, supra n. 57, page 405.

Thus, their legal basis may be found in legislation (mutual legal assistance legislation, legislation on international cooperation, including cross-border use of special investigative techniques such as surveillance and undercover operations, criminal procedure code, specific legislation on joint investigations) or administrative guidelines, standard-operating procedures, long-standing cooperative practices and agreements on a case-by-case basis.

The extent of legislation required depends on the joint investigation model used. In practice, two models have been developed for joint investigations: the first model consists of parallel and coordinated investigations, which are non-co-located, but where the parties have established a common goal and are assisted by law enforcement cooperation as well as the formal MLA process. The officials involved are non-co-located and are enabled to work jointly on the basis of long-standing cooperation practices and/or existing MLA legislation, depending on the nature of the legal system(s) involved.

The second model is an integrated model which can be further characterized as either passive or active one, depending on the extent of law enforcement powers available to participating officers. An example of an integrated/passive team could include the situation where a foreign law enforcement officer is integrated with officers from the host state as an advisor or consultant or, as a technical assistant to the host state. An integrated/active team would include officers from at least two jurisdictions having an ability to exercise (equivalent or at least some) operational powers under the host state control in a defined territory or jurisdiction.

Particular problems relating to the establishment of joint investigations in specific areas of criminal activity include, inter alia, the following: lack of contact points for joint investigations; lack of clarity in determining the officials competent to authorize joint investigations; the necessity for trust, commitment and development of common goals; the need to consider availability of resources and the demand for operational planning including management structures; ensuring the security of operational information; and the need for appropriate training of criminal justice officials.

With regard to the international instruments dealing with joint investigation teams (JITs), Article 19 of the UNTOC encourages, but does not require, the states to formulate agreements or arrangements to establish joint investigative bodies in relation to matters which are the subject of investigations, prosecutions, proceedings in more than one state. In addition, in the absence of such agreements, States are encouraged to seek to establish a legal basis for cooperation on a case-by-case basis, subject to the national sovereignty of the State hosting the joint investigation. The UNCAC also contains a similar provision (Article 49).

At the European Union level, reference to joint investigation was made, for example, in the Treaty of Amsterdam<sup>101</sup> and developed further during the special meeting of the European Council in Tampere.<sup>102</sup>

<sup>101</sup> For the historical evolution of the joint investigation teams, see: *Rijken*, Joint Investigation Teams: principles, practice and problems. Lessons learnt from the first efforts to establish a JIT in *Utrecht Law Review*, vol. 2, issue 2, page 99 et seq.

<sup>102</sup> In this respect, see Conclusion No. 43 of the European Council in Tampere, text available online at: [http://www.europarl.europa.eu/summits/tam\\_en.htm#c](http://www.europarl.europa.eu/summits/tam_en.htm#c).

Currently at the EU level there is a dual legal framework with regard to JITs. Most of the EU Member States<sup>103</sup> have enacted legislation in all related areas in accordance with Article 13 of the EU Convention on Mutual Assistance in Criminal Matters of 2000, which provides a comprehensive framework for the establishment of joint investigation teams.<sup>104</sup> Due to the fact that the ratification process of the EU Convention was too slow, Articles 13, 15 and 16 were then incorporated into a separate EU Council Framework Decision on Joint Investigations adopted in 2002. The Framework Decision was required to be incorporated into the legislation of the EU Member States and was later supplemented by the EU Council Recommendation on a model agreement in 2003 (see below). The Decision will cease to apply when the 2000 Convention shall come into force for all Member States.<sup>105</sup> An almost identical approach with regard to JITs can be found in Article 20 of the Council of Europe Second Additional Protocol to the 1959 European Convention on Mutual Assistance.

Due to its nature and objectives, Eurojust has an overview of joint investigations in the EU as well as relevant joint investigation (operational) agreements. In addition, Eurojust as an organization, or through its national members, is able to request the EU Member States to establish a joint investigation team and/or to participate in such a team. Eurojust is enabled to identify potential cases suitable for joint investigation teams, to facilitate contacts between EU Member States and can organize coordination meetings to discuss the formation of joint investigation teams. Eurojust can also provide support in overcoming language barriers by providing simultaneous translation and can further cooperate with various non-EU countries through contact points and agreements. In 2005, under the aegis of Eurojust, the JITs experts network was created. It meets periodically to exchange information and share best practices, in order to improve the use of JITs at EU level.<sup>106</sup>

Within the European Union context, a model agreement, developed by the EU Council Recommendation of 8 May 2003 and based on the provisions of the EU 2000 Convention, was used as a starting point for negotiations between the relevant national authorities of Member States. Taking into account the need expressed by the practitioners to have an updated model, also acknowledged in the Stockholm Programme,<sup>107</sup> the model agreement has been recently replaced through the Council Resolution of 26 February 2010 on a Model Agreement for setting up a Joint Investigation Team (JIT) (2010/C 70/01).<sup>108</sup> This model distinguishes between general and special conditions. General prerequisites include the following: the parties to the joint investigation (law enforcement agencies, prosecuting authorities), the purpose of the joint investigation, the time frames (and any review dates), identification of the Member State(s) in which the JIT will operate, the State(s) of operation, as well as any specific arrangements of the agreement. With regard to the last point,

<sup>103</sup> Until June 2009, Italy and Greece had not ratified the EU Convention 2000. See, in this respect, the Joint Investigation Teams Manual available in all EU languages at: [http://www.eurojust.europa.eu/jit\\_manual.htm](http://www.eurojust.europa.eu/jit_manual.htm).

<sup>104</sup> More details about the legal framework within EU will be offered further below in the context of the EU Convention 2000.

<sup>105</sup> See the Joint Investigation Teams Manual available in all EU languages at: [http://www.eurojust.europa.eu/jit\\_manual.htm](http://www.eurojust.europa.eu/jit_manual.htm), page 4.

<sup>106</sup> For the list of the conclusions adopted by the Expert Group, see: [http://www.eurojust.europa.eu/jit\\_meetings.htm](http://www.eurojust.europa.eu/jit_meetings.htm).

<sup>107</sup> In this respect, see point 4.3.1 of the Stockholm Programme, available at: [http://www.se2009.eu/polopoly\\_fs/1.26419!menu/standard/file/Klar\\_Stockholmsprogram.pdf](http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf).

<sup>108</sup> The text of the Council Resolution is available at: <http://eurex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:070:0001:0012:EN:PDF>.

the special conditions may include, among others, the following: terms under which seconded members are allowed to participate in or excluded from carrying out investigations or specific conditions under which a seconded member may request his/her own national authorities to take measures requested by the team, without submitting a formal letter of a mutual legal assistance request.

Even though the use of JITs at the EU level was rather slow<sup>109</sup> and there is still a room for improvement, the recent trends have shown that the EU Member States are beginning to reconsider the importance of this form of cooperation, in view of the rapid increase of transnational crime. In the same direction, legal and practical aspects pertaining to joint investigation teams have gained a prominent place in relevant United Nations fora.<sup>110</sup>

---

<sup>109</sup>As of 15 May 2007, only 18 JITs have been set up. See Implementation of the European Arrest Warrant and Joint Investigation Teams at EU and National Level, page 33, available online at: <http://www.statewatch.org/news/2009/feb/ep-study-european-arrest-warrant.pdf>.

<sup>110</sup>See the report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, paragraph 233 (<http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V05/844/09/PDF/V0584409.pdf?OpenElement>) and the report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, paragraph 188 ([http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A\\_CONF.213\\_18/V1053828e.pdf](http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf)).





### III. CONVENTIONS APPLICABLE IN INTERNATIONAL JUDICIAL COOPERATION IN COMBATING IDENTITY-RELATED CRIME AND PRACTICAL ISSUES EMERGING FROM THEIR APPLICATION

#### 1. Importance of identifying the applicable instrument

While dealing with a practical case of identity-related crime, whether it is extradition or mutual legal assistance, it is vital to follow certain steps in order to make sure that the requested State will execute the request accordingly. The first important element which is essential for the execution of the request is to identify the legal instrument applicable in a given case.

The identification of the applicable legal instrument is crucial as it will help the requesting State identify essential information related to the procedure. In an extradition case, the requesting State will, for example, based on the applicable convention or bilateral treaty, manage to identify:

- The period of time within which the request and the additional documents have to be submitted—in case the person was provisionally arrested with a view to extradition;
- The annexed documents that need to be attached and other procedural requirements that need to be met;
- The channels and means of communication;
- The relationship with other relevant international instruments. In particular, in those cases where both a bilateral treaty and a multilateral treaty dealing with extradition are in force and are applicable, the judicial authority of the requesting State shall know which one to apply;<sup>111</sup>
- The language in which the request has to be submitted to. Normally, this is the official language of the requested State. If that State has more than one official language, only one of them can be chosen. Some countries can also accept languages other than their own.<sup>112</sup>

The same applies to MLA requests. Identifying the applicable treaty will be essential in defining the steps that need to be taken for the transmission of the relevant request. If a given type of MLA request is allowed by that treaty, the next steps will be formulating the

<sup>111</sup>The European Convention on Extradition 1957, for example, stipulates in Article 28 that the Convention will “supersede the provisions of any bilateral treaties, conventions or agreements governing extradition between any two Contracting Parties” while other conventions such as Council of Europe Convention on Cybercrime in Article 39, paragraph 2, is conferring pre-eminence to pre-existent instruments.

<sup>112</sup>This is a very useful provision (especially for urgent cases), which is normally promoted by those countries which have rare languages. Therefore allowing the requesting state to find a translator into a language, popular at European level, such as English or French, is relatively easier. Usually, each state makes a declaration to the applicable legal instrument stating which languages it will accept.

request, choosing the channels and means of communication, languages and deadlines.<sup>113</sup> In cases of identity-related crime having a transnational nature, several international and regional instruments may be applicable.<sup>114</sup>

Bearing in mind the above points, a summary of legal instruments applicable at regional or international level shall be presented below. The summary does not constitute an exhaustive list, but a mere exemplification of the legal tools that can be used in international cooperation cases involving identity-related crimes. Some of these instruments are focused only on one specific field of cooperation (for example, extradition or mutual legal assistance), while others, such as the UNTOC or the Council of Europe Convention on Cybercrime,<sup>115</sup> contain provisions on international cooperation in criminal matters. In addition, there are various bilateral treaties, which, for practical reasons, cannot be discussed in detail in the present guide.

## 2. Conventions applicable with regard to the extradition procedure

The following overview presents a brief summary of regional instruments on extradition, as well as multilateral instruments containing provisions on extradition, which are of relevance in cases of identity-related crime. By indicating the online resources they can be found at and highlighting their relevance. The guide will provide more analytical information on the UNTOC and the Council of Europe Cybercrime Convention.

### *Regional extradition instruments*

#### European Convention on Extradition, 1957 and its additional Protocols

The Convention and its two additional protocols (1975 and 1978) represent very useful tools in this matter between the European Member States of the Council of Europe, despite the fact that the “mother” Convention dates back to 1957.

<sup>113</sup>As an example, one may offer a case of summoning an accused person that needs to be present at trial. Some countries require that the request to be submitted with sufficient time prior the settled term of the trial, to allow themselves time to transmit the documents to that person before the specified term. At European level many states have made declarations to Article 7(3) of the Council of Europe Convention on mutual assistance in criminal matters, 1959 which allows for parties to establish a term within the issuing state should transmit the documents that need to be served: so the term shall not exceed 50 days. According to the Explanatory Report of the Convention, this provision was a compromise of the legal systems existent at European level, some of them not allowing a judgment to be rendered in absentia.

<sup>114</sup>See, for instance, the practical examples offered by Romania as a response to the questionnaire issued by the PC-OC on Mutual Legal Assistance in Computer-Related Cases, PC-OC (2008) 08, available at: <http://www.coe.int/tcj> (with reference to the multitude of agreements needed to summon the injured parties located in different states on different continents).

<sup>115</sup>Council of Europe Convention on Cybercrime (CETS No. 185), available at: <http://conventions.coe.int>. For more details see: *Sofaer*, Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: [http://media.hoover.org/documents/0817999825\\_221.pdf](http://media.hoover.org/documents/0817999825_221.pdf); *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, *Computer Law Review International*, 2006, page 140 et seq.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, *Computer Law Review International* 2008, page 7 et seq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, *Entertainment Law Review*, 2002, No. 1, available at: <http://elr.lls.edu/issues/v23-issue1/aldesco.pdf>; *Jones*, The Council of Europe Convention on Cybercrime, *Themes and Critiques*, 2005, available at: <http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf>; *Broadhurst*, Development in the global law enforcement of cyber-crime, in *Policing: An International Journal of Police Strategies and Management*, 29(2), 2006, page 408 et seq.

The Convention mentions in Article 2 that the extraditable offences shall be those punishable under the laws of both the requesting and requested States by deprivation of liberty or under a detention order for a maximum period of at least one year. In case a sentence has already been pronounced, the punishment disposed must be for at least 4 months. The extradition is to be refused with regard to military and political offences or if there are substantial grounds to believe that the person sought was discriminated against.<sup>116</sup> On the other hand, fiscal offences can become extraditable offences, if the parties agree thereto (prior agreement is therefore necessary). Also, the extradition of nationals can be refused, the nationality being determined at the time of making the decision concerning the extradition.<sup>117</sup> In case the requested party does not extradite its nationals, the Convention establishes the obligation for the requested State to take over the procedure. Article 9 tackles the problem of *ne bis in idem* with regard to final judgments. Some adjustments to it are brought by the Additional Protocol to the European Convention on Extradition, adopted in 1975. The Protocol supplements Article 9 by applying the principle to the extradition of a person against whom a final judgment has been rendered in a third State.

The communication of the documents is to be made, as a general rule, through diplomatic channels.<sup>118</sup> The term of the provisional arrest (within which the extradition should be submitted) is 18 days and in any case cannot exceed 40 days.<sup>119</sup> The provisions of the Convention supersede any other pre-existent bilateral treaties, conventions or agreements applicable between two parties. Yet, new bilateral or multilateral agreements can be concluded between the parties in order to supplement the provisions of the Convention or to facilitate the application of its principles.<sup>120</sup>

The Second Additional Protocol, adopted in 1978, brings changes to Article 5 relative to fiscal offences and also supplements Article 3 by introducing the concept of judgment *in absentia* in order to correspond to the situations encountered in practice. Another important change is brought to Article 12, which allows States parties to establish a direct contact between their ministries of justice for extradition purposes. Then again, transmission through diplomatic channels is allowed.

In practice, many countries accept the transmittal of documents via fax, with subsequent formal confirmation through post (if a direct contact between the ministries of justice is permitted) or through diplomatic channels.

### Inter-American Convention on Extradition, 1981<sup>121</sup>

The Convention was developed under the auspices of the OAS and is the current regional agreement in this field. The Convention gives priority to multilateral or bilateral treaties concluded by the state parties earlier, unless the parties have decided

<sup>116</sup> See Articles 3 and 4 of the Convention.

<sup>117</sup> See Article 6, *idem*.

<sup>118</sup> See Article 12, *idem*.

<sup>119</sup> Some countries require the submittal of the documents in 18 days, others accept their prolongation up to 40 days.

<sup>120</sup> See Article 28 of the Convention.

<sup>121</sup> The Convention and the list of States parties are available online at: <http://www.oas.org/juridico/treaties/b-47.html>.

otherwise.<sup>122</sup> It contains all the relevant provisions referring to the extradition procedure, addressed in the previous pages.

It should be pointed out that extraditable offences have to be punished under the laws of both the requesting and requested States with at least two years of imprisonment and, when the extradition is requested for the execution of a sentence, the duration of the sentence still to be served has to be of at least six months (note that the thresholds are higher than in the case of Council of Europe Convention). Another important element is the fact that the nationality of the person sought may not be invoked as a ground to deny the extradition, except when the laws of the executing state provide otherwise. The grounds of refusal are mentioned in Article 4. Although transmission of the extradition request as a general rule shall be made through diplomatic channels, a direct transmission from government to government is not excluded if such a procedure has been agreed upon by the parties concerned.

### The London Scheme for Extradition within the Commonwealth<sup>123</sup>

This Scheme includes the amendments brought in November 2002 in Kingston and comprises provisions specific to common law countries, but also general principles which are to be found in any extradition arrangement. As such, it defines the extraditable offences and provides for a broad interpretation of the double criminality check.<sup>124</sup> Fiscal offences and offences committed outside the territory of the requesting State are included in the list of extraditable offences (clause 2). The Scheme also contains references to the provisional warrants, and the hearing of the case which will take place as if the person were charged with an offence in the requested State. The details with regard to the evidence that needs to be submitted before the court, including those that can establish a prima facie case, are to be found in clauses 5 (Committal Proceedings) and 6 (Optional Alternative Committal Proceedings).

On the subject of grounds of refusal, clause 12 (Political Offence Exception) establishes as a rule the refusal to execute extradition requests with reference to political offences. There are situations in which this rule is not followed though, such as those where multilateral international conventions impose an obligation on the States parties to extradite or prosecute or where the political offence ground of refusal is not applicable under international law. Other mandatory grounds of refusal include discrimination, ne bis in idem, or the trivial nature of a case (see for more details clauses 12 and 13).

Among the optional grounds of refusal, the following should be mentioned: judgements rendered in absentia in the requesting State, immunity from prosecution due to lapse of

<sup>122</sup>Article 33 of the Convention entitled Relations with other Conventions on Extradition states as follows: “This Convention shall apply to the States parties that ratify it or accede to it and shall not supersede multilateral or bilateral treaties that are in force or were conducted earlier unless the States parties concerned otherwise expressly declare or agree, respectively. The States parties may decide to maintain in force as supplementary instruments treaties entered into earlier”. This could lead for example to appliance of the Montevideo Convention on Extradition, 1933, which was a previous regional initiative. For more details with regard to the relevant instruments in the region, see *Gilbert*, *Transnational Fugitive Offenders in International Law, Extradition and other Mechanisms*, supra n. 49.

<sup>123</sup>The text of the Scheme can be found online at: [http://www.thecommonwealth.org/shared\\_asp\\_files/uploaded\\_files/%7B56F55E5D-1882-4421-9CC1634DF17331%7D\\_London\\_Scheme.pdf](http://www.thecommonwealth.org/shared_asp_files/uploaded_files/%7B56F55E5D-1882-4421-9CC1634DF17331%7D_London_Scheme.pdf). The origins of the Commonwealth cooperation date back to 1843 when the first statute referring to the surrender of fugitives was established. For details see *Bassiouni*, *International Extradition, United States Law and Practice*, 5th ed., Oceana, 2007, pages 21-71.

<sup>124</sup>See clause 2, Extradition offences and dual criminality rule, paragraph 3a) and b), *ibid*.

time or amnesty, the military nature of the offence, extraterritoriality, death penalty and nationality (see clauses 14 and 15). Alternative measures are also applicable when extradition is refused to ensure that States parties are not used as safe havens from justice (clause 16).

The competent authorities include a judicial authority competent to hear the extraditable person and an executive authority responsible for orders for extradition. The speciality rule is stipulated in clause 20.

### The Southern African Development Community (SADC) Protocol on Extradition, 2002<sup>125</sup>

The Protocol contains provisions referring to extraditable offences, provisional arrest, the speciality rule and simplified extradition procedure. With regard to the extraditable offences, according to Article 3 of the Protocol, the extradition can be required for offences punishable under the laws of both the requesting and requested States by a punishment of at least one year. In cases where the extradition is sought for the enforcement of the sentence, at least six months of the sentence must remain to be served. Among the mandatory grounds of refusal mentioned in Article 4 are those related to political and military offences, discrimination, *ne bis in idem*, and immunity (lapse of time and amnesty included). In the list of the optional grounds of refusal the Protocol includes the nationality of the person sought (if that person is a national of the requested State) and the death penalty (if the offence for which the extradition is requested is punished by death penalty in the requesting State). The extradition requests must be submitted through diplomatic channels to the Ministries of Justice or other authorities designated by the States parties. The maximum term of the provisional arrest is 30 days.

### The Arab League Extradition Agreement, 1952/Riyadh Arab Agreement for Judicial Cooperation, 1983

This Convention was approved by the League of Arab States in 1952, but ratified only by Egypt, Jordan and Saudi Arabia.<sup>126</sup>

The list of ratifications/accessions was later extended.<sup>127</sup> The Convention, similar to other instruments in the field, contains provisions allowing for the continuation in the application of the pre-existent bilateral treaties<sup>128</sup> between States parties, and in case of conflict, the instrument that best facilitates the extradition of the person sought will prevail.

The Convention does not comprise a list of extraditable offences, but applies the punishment criteria. The crime has to be punishable by at least one year imprisonment, or, if the extradition is sought for the execution of a sentence, the imprisonment imposed has to be of minimum two months.

<sup>125</sup> The Protocol is available online at: <http://www.sadc.int/index/browse/page/148>.

<sup>126</sup> See *Bassiouni*, International Extradition, United States Law and Practice, supra n. 123 in fine, page 20.

<sup>127</sup> For details, see *Gilbert*, Responding to International Crime, Koninklijke Brill NV, 2006, page 32.

<sup>128</sup> For more details on the Convention, see *Shearer*, Extradition in International Law, Manchester University Press, 1971, pages 52-53.

Impediments to the extradition under the Agreement include political offences, statute of limitations applicable in the requesting State and non-extradition of nationals (but in this case, the requested State is obliged to initiate domestic proceedings in lieu of extradition).

Another relevant instrument in this geographical context is the Riyadh Arab Agreement for Judicial Cooperation (1983), which is applied by a greater number of Arab States, thus having a more extended geographical applicability.<sup>129</sup>

As its very title indicates, the Convention has a wider field of application, tackling international cooperation in criminal matters in general, and, in this context, deals with extradition in Part VI—Extradition of Accused or Convicted Persons.<sup>130</sup>

The threshold of the penalty is at least one year. Grounds of refusal are established in Article 41 (political, military offences, ne bis in idem, amnesty, if the crime for which the extradition was sought is committed in the territory of the requested State, etc.). Nationality is an optional ground of refusal. The formal requirements for submitting the extradition request appear in Article 42. The regional instrument allows for a provisional arrest in anticipation of the extradition request, the period within which the person can be provisionally detained until the documents are received is 30 days. Other provisions deal with supplementary information, multiple requests, speciality rule, etc.

It is also important to mention that the Arab League States have concluded other regional and bilateral agreements that could also present relevance in the field of international cooperation in criminal matters.<sup>131</sup>

### Other relevant conventions

There are also other regional conventions referring to extradition which should be noted here. Among those conventions are the Nordic States Scheme, in force through the adoption of the Act on Extradition for Criminal Offences to Denmark, Finland, Iceland and Norway in 1962,<sup>132</sup> the Benelux Convention on Extradition and Judicial Assistance in Penal Matters (1962),<sup>133</sup> and the ECOWAS<sup>134</sup> Convention on Extradition adopted in 1994.<sup>135</sup>

At the EU level, prior to the adoption of the European arrest warrant system, two other instruments, aiming at facilitating the extradition process among the EU Member States, were adopted: the Convention on Simplified Extradition Procedure between the Member

<sup>129</sup>For more information about the applicability of this Convention, see *Gilbert*, Responding to International Crime, supra n. 127.

<sup>130</sup>The text of the Convention is available in English at: <http://www.unhcr.org/refworld/type.MULTILATERAL.TREATY.ARAB.3ae6b38d8.0.html>.

<sup>131</sup>For a list of relevant instruments, see *Ibrahim/Siam*, An Overview of the Arab Guiding Law on International Cooperation in Criminal Matters, *Revue Internationale de Droit Pénal*, vol. 76, 2005, pages 105–106.

<sup>132</sup>*Bassiouni*, International Extradition, *United States Law and Practice*, supra n. 126, page 23.

<sup>133</sup>The Benelux Convention was concluded in 1962 between Belgium, Netherlands and Luxembourg when none of the mentioned states had ratified the Council of Europe Convention on Extradition of 1957, see *Mathisen*, Nordic Cooperation and the European Arrest Warrant: Intra-Nordic Extradition, the Nordic Arrest Warrant: Intra-Nordic Extradition, the Nordic Arrest Warrant and Beyond, in *Nordic Journal of International Law*, 79 (2010), page 4.

<sup>134</sup>ECOWAS is the abbreviation for the Economic Community of West African States.

<sup>135</sup>*Bassiouni*, International Extradition, supra n. 126, page 24.

States of the European Union (1995)<sup>136</sup> and the Convention Relating to Extradition Between the Member States of the European Union (1996).<sup>137</sup>

*International and regional instruments dealing, among others aspects, with extradition*

### United Nations Convention against Transnational Organized Crime (UNTOC), 2000

The relevant provisions related to extradition are reflected in Article 16 of the Convention<sup>138</sup> and represent a valuable tool for countries from different parts of the world that have not concluded bilateral agreements or arrangements on extradition.

#### *Scope of application*

Article 16(1) of the UNTOC defines the scope of the obligation OF States parties to extradite by providing that an extradition request is to be granted, subject to the double criminality requirement, with respect to “the offences covered by this Convention or in cases where an offence referred to in Article 3, paragraph 1 (a) or (b), involves an organized criminal group and the person who is the subject of the request for extradition is located in the territory of the requested Party...”. Consequently, the extradition obligation applies initially to the Convention offences, serious crimes punishable by a maximum deprivation of liberty of at least four years or a more severe penalty, as well as to the Protocol offences (see Article 1(2) of each of the Protocols supplementing the parent Convention), provided that they are transnational in nature and involve an organized criminal group.<sup>139</sup> However, and always subject to the dual criminality requirement, the extradition obligation also applies in cases where these offences involve an organized criminal group and the person whose extradition is requested is simply located in the territory of the requested State, without being necessary transnationality of the criminal conduct to be established. In this sense, the scope of application of Article 16 of the UNTOC is broader than the scope of application of the Convention itself, since this provision could also be applicable in cases where the offender is simply apprehended in the territory of another State Party.<sup>140</sup>

#### *Legal basis for extradition*

As previously stated, the Convention can be used as a legal basis by those States that make the extradition conditional on the existence of a treaty and have not concluded

<sup>136</sup>The Convention was published in the Official Journal of the European Communities, C078, 30 March, 1995 and has as its purpose the facilitation of the extradition between Member States in supplementing the application of the Council of Europe 1957 Convention on Extradition, avoiding by that the formal extradition procedures and reducing the delays. More information about its applicability is available at: [http://europa.eu/legislation\\_summaries/justice\\_freedom\\_security/judicial\\_cooperation\\_in\\_criminal\\_matters/114015a\\_en.htm](http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/114015a_en.htm); see also *Bantekas/Nash*, International Criminal Law, supra n. 58, pages 314-315.

<sup>137</sup>The Convention was published in the Official Journal of the European Communities, C313, 23 October 1996. More information about the applicability of the Convention is available at: [http://europa.eu/legislation\\_summaries/justice\\_freedom\\_security/judicial\\_cooperation\\_in\\_criminal\\_matters/114015b\\_en.htm](http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/114015b_en.htm); see also *Bantekas/Nash*, supra n. 57, page 315 et seq.

<sup>138</sup>The status of ratification of the UNTOC and its supplementary Protocols can be found at: <http://www.unodc.org/unodc/en/treaties/CTOC/signatures.html>.

<sup>139</sup>See the Legislative Guide for the United Nations Convention against Transnational Organized Crime, page 197 et seq., available at: [http://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html#\\_Full\\_Version\\_1](http://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html#_Full_Version_1).

<sup>140</sup>In this sense, see paragraph 5 of the Report of the Chairperson on the Meeting of the open-ended working group of Government experts on international cooperation, Vienna, October 2008, CTOC/COP/2008/18, available at: [http://www.unodc.org/documents/treaties/organized\\_crime/Report\\_of\\_the\\_Chair\\_English.pdf](http://www.unodc.org/documents/treaties/organized_crime/Report_of_the_Chair_English.pdf).

any extradition treaty. The Convention can also be used by those countries that already apply existing bilateral treaties, based on “the list” criteria. In these cases, the Convention could be applied by States parties in lieu of their bilateral arrangements, proving its usefulness.<sup>141</sup> In any case, the extradition shall be subject to the conditions provided by the law of the requested State, or applicable extradition treaties, including the minimum penalty requirement or the grounds of refusal.<sup>142</sup>

#### *Specific provisions*

Article 16(9) establishes the basis for the provisional arrest with a view to extradition. In addition, UNTOC provides guarantees for the sought person<sup>143</sup> and prohibits the denial of extradition for fiscal offences.<sup>144</sup>

A series of provisions in Article 16 reflect the fact that the reluctance to extradite their own nationals appears to be lessening in many States. In cases where the requested State refuses to extradite a fugitive on the grounds that the fugitive is its own national, the State is often seen to have an obligation to bring the person to trial. This is an illustration of the principle of *aut dedere aut judicare* (extradite or prosecute).<sup>145</sup> The provision refers to the possibility of temporary surrender of the fugitive on condition that he or she will be returned to the requested State party for the purpose of serving the sentence imposed.<sup>146</sup> Where extradition is requested for the purpose of enforcing a sentence, the requested State may also enforce the sentence that has been imposed in accordance with the requirements of its domestic law.<sup>147</sup>

With regard to human rights in extradition proceedings, the Convention imposes certain standards to assure the right to a fair trial and that no discrimination based on a person’s sex, race, religion, nationality, ethnic origin or political opinion can occur. The working group on international cooperation, established by the Conference of the Parties to the UNTOC,<sup>148</sup> has acknowledged that currently there are different practices on the guarantee assurances applicable among States, but despite these different approaches, the guarantees given by the authorized agencies should be considered valid and trustworthy.<sup>149</sup>

Serious consideration should be given to the issue of judgments rendered in absentia in the requesting State. When this issue arises, the circumstances under which such a judgment was rendered and possible retrial guarantees should be presented to the requested State in as much detail as possible.<sup>150</sup>

In respect of fiscal offences, as mentioned earlier, States parties are not permitted to deny extradition and are obliged to ensure that such a ground of refusal is not included

<sup>141</sup> Paragraph 5, *ibid.*

<sup>142</sup> See Article 16(7).

<sup>143</sup> See Article 16(13) and (14), *ibid.*

<sup>144</sup> Paragraph 15, *idem.*

<sup>145</sup> See Article 16(10).

<sup>146</sup> See Article 16(11).

<sup>147</sup> See Article 16(12).

<sup>148</sup> For the work of this Group, see: <http://www.unodc.org/unodc/en/treaties/working-group-on-international-cooperation.html>.

<sup>149</sup> See, in this sense, paragraph 18 of the CTOC/COP/2008/18, *supra* n. 140.

<sup>150</sup> Paragraph 17, *ibid.*



in their laws or treaties. This may require the adoption of new instruments or the amendment of domestic legislation to that effect.<sup>151</sup>

Last but not least, the Convention asks for consultations between the requested and the requesting States, before refusing an extradition request, a measure which allows the requesting State to present supplementary information and expert opinions which could further support the extradition request.<sup>152</sup> This represents an additional guarantee which increases the chances of an extradition request to be actually executed.

### United Nations Convention against Corruption (UNCAC), 2003

This Convention<sup>153</sup> may become relevant if identity-related crimes are linked to corruption offences established in accordance with this instrument.<sup>154</sup> Due to the fact that it could become applicable only incidentally, it shall be briefly presented here with a view to emphasize its connection with the other relevant extradition instruments.

The relevant provisions referring to the extradition are found in Article 44, where similar requirements to those of Article 16 of the UNTOC are foreseen. In accordance with that provision, States parties should seek to expand their extradition treaty network and/or adjust their relevant legislation, thus ensuring the existence of appropriate legal frameworks to facilitate extradition. The UNCAC attempts to set a basic minimum standard for extradition and requires States parties, that make extradition conditional on the existence of a treaty, to indicate whether the Convention is to be used as a legal basis for extradition matters and, if not, to conclude treaties in order to implement Article 44 (Article 44(6)(b)), as well as bilateral and multilateral agreements or arrangements to enhance the effectiveness of extradition (Article 44(18)).

If States parties do not make extradition conditional on the existence of a treaty, they are required by the Convention to use extradition legislation as legal basis for the surrender of fugitives and recognize the offences falling within the scope of the Convention as extraditable offences between themselves (Article 44(7)).

It is important to note that despite the fact that the double criminality is imposed as a main rule among the conditions for requiring an extradition (see Article 44(1) of the UNCAC), the Convention also allows for the lifting of the double criminality requirement by stipulating that a State party, whose law so permits, may grant the extradition of a person for any of the offences covered by the Convention which are not punishable under its own domestic legislation (see Article 44(2)). This represents a progressive measure which is not provided for in the UNTOC.

<sup>151</sup> See Legislative Guide, page 224, supra n. 139.

<sup>152</sup> See Article 16(16).

<sup>153</sup> The status of ratification of the UNCAC can be found at: <http://www.unodc.org/unodc/en/treaties/CAC/signatories.html>.

<sup>154</sup> The offences enshrined in the Convention are to be found in Articles 15 to 25 of the Convention (bribery of national public officials, bribery of foreign public officials and officials of public international organizations, embezzlement, misappropriation or other diversion of property by a public official, trading in influence, abuse of functions, illicit enrichment, bribery in the private sector, embezzlement in the private sector, laundering of proceeds of crime, concealment, and obstruction of justice).

The UNCAC allows for expedited procedures, simplified evidentiary requirements and legislative changes, if needed, to correspond to the standards of the Convention. It further includes the *aut dedere aut judicare* principle, temporary surrender and taking over the execution of the sentence as alternatives in cases extradition is denied on the ground of nationality.<sup>155</sup>

Generally, the extradition provisions are designed to ensure that the Convention supports and complements existing extradition arrangements and does not depart from them.

### Council of Europe Cybercrime Convention, 2001

Extradition is regulated by Article 24 of the Council of Europe Convention on Cybercrime.<sup>156</sup> The article stipulates that the crimes established in accordance with Articles 2-11 of the Convention are extraditable offences as long as they are punished under the laws of both the requesting and requested States by deprivation of liberty of at least one year. Reiterating the provisions of Article 23, the Convention confers pre-eminence to other instruments as regards the quantum of the punishment, if such conventions or bilateral treaties are applicable between the requesting and requested States. With regard to Member states of the Council of Europe, the European Convention on Extradition could have priority.

The Convention on Cybercrime enables States parties to consider it as a legal basis for extradition with respect to any offences covered by its scope of application if they make extradition conditional on the existence of a treaty. Parties that do not make extradition conditional on the existence of a treaty should recognize the criminal offences established by the Convention as extraditable offences between themselves. In general, extradition is subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

Paragraph 6 of Article 24 provides for the application of the *aut dedere aut judicare* principle to enable the initiation of domestic proceedings in the requested State in lieu of extradition of a national of that State. It is important to remember though that the Convention requires a specific request from the requesting State to the requested State to take over the proceedings.<sup>157</sup>

Finally, Article 24 requires each of the States parties to designate an authority competent to receive and make extradition requests and requests for provisional arrest with a view to extradition, in the absence of an applicable treaty.

<sup>155</sup>For more details on the application of UNCAC, see The Legislative Guide for the Implementation of the United Nations Convention against Corruption, page 178 et seq., available at: [http://www.unodc.org/documents/treaties/UNCAC/Publications/LegislativeGuide/06-53440\\_Ebook.pdf](http://www.unodc.org/documents/treaties/UNCAC/Publications/LegislativeGuide/06-53440_Ebook.pdf).

<sup>156</sup>Council of Europe Convention on Cybercrime, supra n. 117. For more details, see: *Sofaer*, Toward an International Convention on Cyber Security, *ibid*; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, *ibid*, page 140 et seq.; *Gercke*, National, Regional and International Approaches, *ibid*; *Aldesco*, The Demise of Anonymity..., *ibid*; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, *ibid*; *Broadhurst*, Development in the global law enforcement of cybercrime, *ibid*.

<sup>157</sup>See the Explanatory Report to the Council of Europe Cybercrime Convention, paragraph 251, available at: <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

### 3. Conventions applicable with regard to traditional forms of MLA

On the subject of mutual legal assistance, the Cybercrime Convention introduced some new forms of cooperation with regard to crimes committed in cyberspace, which allow Member States to cooperate on a real-time basis. The presentation of the relevant provisions referring to mutual assistance will concentrate firstly and extensively on traditional forms of mutual legal assistance and the specific forms of cooperation introduced by Council of Europe Cybercrime Convention will be introduced in a separate subchapter.

Despite the fact that most of the conventions presented are regional ones, enumerating their main elements can provide practitioners located in other regions with an overview about main elements necessary to formulate a request to a particular country. The following subsections are not intended to provide an exhaustive list of conventions and their detailed provisions, but only to give a picture of some instruments relevant to the mutual legal assistance in cases involving identity-related crimes.

#### *United Nations Convention against Transnational Organized Crime (UNTOC), 2000*

The main provision dealing with MLA is Article 18 of UNTOC, however, other provisions are relevant as well (see, for example, Article 13 of the UNTOC on international cooperation for purposes of confiscation, Article 19 on joint investigations and Article 20 on special investigative techniques).

##### *Scope of application*

The scope of the application of Article 18 of the UNTOC which governs mutual legal assistance is broader than the scope of application of the Convention itself. According to paragraph 1 of this article, States parties are required to provide “the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by the Convention”. In addition, States parties are also obliged to “reciprocally extend to one another similar assistance” where the requesting State has “reasonable grounds to suspect” that one or some of the offences are transnational in nature, including that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State party, and that they involve an organized criminal group.

It is evident that Article 18 sets a lower evidentiary standard, as compared to Article 3 of the UNTOC on its scope of application, requiring only reasonable possibility and not evidence based on facts with respect to transnationality and involvement of organized criminal group. The lower evidentiary threshold is intended to facilitate mutual legal assistance requests for the purpose of determining whether the elements of transnationality and organized crime are present in a certain case, and whether international cooperation may be necessary and may be sought under the Convention for subsequent investigative measures, prosecution or extradition.

The offences to which the MLA request refers should be covered by Articles 5, 6, 8 and 23 of the UNTOC or should constitute a serious crime<sup>158</sup> on the condition that the offence for which assistance is requested is transnational in nature<sup>159</sup> and involves an organized criminal group.<sup>160</sup>

With regard to identity-related crime, the UNTOC, in general, is only applicable if the offence is considered to be a serious crime, which can be the case depending on the circumstances of the offences.<sup>161</sup> With regard to the required transnational dimension, it should be reiterated that this requirement is partially lifted in Article 18 of the Convention if the victims, witnesses, proceeds, instrumentalities or evidence are located in the requested State.<sup>162</sup> In order to comply with the request of the requesting State, some countries may refer to the principle of double criminality. This is an optional condition and does not impede the requesting State to grant assistance irrespective of this.<sup>163</sup> The UNTOC provisions related to MLA can also apply with regard to the offences criminalized by the three supplementary protocols.<sup>164</sup>

#### *Grounds for refusal*

Referring to the grounds of refusal of assistance, bank secrecy cannot be invoked as such a ground.<sup>165</sup> Apart from the double criminality requirement, there are some other optional grounds of refusal mentioned in paragraph 21: non-conformity with the provisions of UNTOC, nonconformity with the provisions of the legal system of the requested state, sovereignty, *ordre public*, security, other essential interests, or impediments to execute a certain action emerging from the domestic law of the requested State and that would apply for a similar offence had it been the subject of criminal proceedings in its own jurisdiction. The Convention establishes that any refusal to execute a MLA request shall be reasoned<sup>166</sup> and in any case, consultations shall take place between the requested and requesting States before refusing a request to consider whether assistance may be granted subject to such terms and conditions as may be deemed necessary.<sup>167</sup>

<sup>158</sup> According to Article 2(b) of the UNTOC, “a serious crime shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty”.

<sup>159</sup> According to Article 3(2) of the UNTOC a crime is considered to be transnational if:

- (a) it is committed in more than one state;
- (b) it is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
- (c) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or
- (d) It is committed in one State but has substantial effects in another state.

<sup>160</sup> See Article 3(1)(b) of the UNTOC. Also, for the definition of the organized criminal group see Article 2(a) according to which “organized criminal group shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offence established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit”.

<sup>161</sup> See the Report of the Second Meeting of the Core Group of Experts on Identity-Related Crime, Vienna, 2-3 June 2008, in which it was noted that “identity-related crime per se was not expressly mentioned in the text of the Convention, but two closely-related offences, participation in an organized criminal group and money-laundering, were specifically established by that instrument. Furthermore, other offences such as identity theft, identity fraud, trafficking in identity information or documents and conventional economic fraud would fall within its scope of application for purposes of investigation and prosecution if they were criminalized as ‘serious crimes’ within the meaning of Article 2” -E/CN.15/2009/CRP.11.

<sup>162</sup> See Catalogue of examples of cases of extradition, mutual legal assistance and other forms of international legal cooperation on the basis of the United Nations Convention against Transnational Organized Crime, 17 September 2008, CTOC/COP/2008/CRP.2, page 2.

<sup>163</sup> See Article 18(9) of the UNTOC.

<sup>164</sup> For the interpretation of the scope, see Legislative Guide, supra n. 139, page 220 et seq.

<sup>165</sup> See Article 18(8).

<sup>166</sup> See Article 18(23).

<sup>167</sup> See Article 18(26).

*Types of mutual legal assistance allowed by the Convention*

The Convention permits a wide range of mutual legal assistance requests, starting from taking evidence or statements, service of judicial documents, executing searches, seizures, freezing, providing information, to any type of assistance which is not contrary to the domestic law of the requested State.<sup>168</sup>

*Content of the request and other formal requirements*

The content of the request is clearly stipulated in paragraph 15 of Article 18. The elements required include the identification of the authority making the request, the subject matter, a summary of the relevant facts, a description of the assistance sought, the identity of the person concerned and, if available, his/her whereabouts. The request has to be executed according to the domestic provisions of the requested State. However, it is also provided that, to the extent not contrary to the domestic law of the requested State and where possible, the request shall be executed in accordance with the procedures specified in the request (Article 18(17)). The UNTOC encourages direct contact and consultations in order to assure a higher degree of admissibility in the requesting State of evidence gathered in the requested State. Special attention should also be given to the confidentiality requirements.<sup>169</sup>

*Channels and means of communication*

With regard to channels of communication, the UNTOC requires that MLA requests are transmitted from a central authority to a central authority,<sup>170</sup> underscoring through its provisions the importance of a speedy and proper execution of the request. The role of central authorities can differ from one country to another, in some being directly involved in handling the requests, in others only forwarding such requests. The Convention leaves it to the States whether to require the transmittal through diplomatic channels. With respect to the speed of international cooperation, it is unfortunate that many countries still employ this method. As a consequence, the responses from the competent authorities do not arrive in proper time, as it could take more than six months until a response is received. In cases of urgency, the use of the International Criminal Police Organization (Interpol) is allowed where the States parties agree. Oral requests are allowed only in urgent circumstances and need to be followed by a written request. In order to identify the channels and means of communication used by a certain requested State, it is recommended to use the online directory of competent authorities or the printed format made available by the United Nations.

The reports of States parties concerning the application of the Convention demonstrate that, while many States have legislation requiring the MLA requests to be made in writing, only several countries reported transmission in advance of temporary requests via e-mail.<sup>171</sup>

*Spontaneous transmission of information*

Paragraphs 4 and 5 of Article 18 provide a legal basis for a State party to forward to another State party information or evidence it believes is important to combat offences

<sup>168</sup> See Article 18(3).

<sup>169</sup> See CTOC/COP/2008/18, supra n. 140, paragraphs 33, 34.

<sup>170</sup> See Article 18(13).

<sup>171</sup> See CTOC/COP/2008/18, supra n. 140, paragraph 27.

covered by the Convention and the Protocol, where the other country has not made a request for assistance and may be completely unaware of the existence of such information or evidence. The aim of these provisions is to encourage (no obligation is imposed) States to exchange information on criminal matters regardless of a prior request. The receiving State may well use the information provided subsequently in order to submit a formal request for assistance. The only general obligation imposed for the receiving State, which is similar to the restriction applied in cases where a request for assistance has been transmitted, is to keep the information transmitted confidential and to comply with any restrictions on its use, unless the information received is exculpatory to the accused person. In this case the receiving State can freely disclose this information in its domestic proceedings. In balancing the need to keep the information confidential and the right of the accused to prove his innocence, the Convention has evidently given priority to the latter.

#### *Relationship with other instruments*

In order to formulate a mutual legal assistance request for an identity-related crime based on the UNTOC, there are several considerations to bear in mind, including the clarification whether any other legal instrument is applicable between the requesting and the requested States. Article 18(6) stipulates that the UNTOC shall not affect the obligation undertaken under any other previous or future bilateral or multilateral treaty that would govern in whole or in part the issue of mutual legal assistance. Article 18(7) enables States parties to apply the provisions of the article as a self-standing and complete MLA treaty applicable between them if they are not bound by bilateral arrangements. Thus, paragraphs 9-29 of Article 18 are applicable for States that have not concluded any previous treaty or agreement. If a treaty is already in force between the States parties concerned, the rules of this treaty shall apply instead, unless the parties agree to apply the rules and requirements set forth in paragraphs 9-29. States parties are also strongly encouraged, but not obliged, to apply any of these paragraphs, if they facilitate cooperation.<sup>172</sup>

It should be noted that Article 18(30) enables States parties to conclude bilateral agreements or arrangements that would give practical effect to the provisions of Article 18.

#### *Summary*

The UNTOC is a very important and useful tool, applicable worldwide. Normally international cooperation is, in fact, regional in character, developed in a specific area between certain countries that have strong economic and cultural links. Transnational crime poses challenges in this respect, as regional instruments are no longer sufficient to cover the full extent of the problem. Identity-related crime represents an example in this regard. The UNTOC has already proved its value as legal basis for international cooperation between countries from different continents.<sup>173</sup> Therefore, if a State has to transmit a request to another State with which is not bound by a regional or bilateral treaty, the first step to make is to check whether that specific

<sup>172</sup>For that interpretation, see CTOC/COP/2008/18, supra n. 140, paragraphs 25 and 26.

<sup>173</sup>See the catalogue of examples of cases of extradition, mutual legal assistance and other forms of international legal cooperation on the basis of the United Nations Convention against Transnational Organized Crime, CTOC/COP/2010/CRP.5/Corr.1.

identity-related crime for which assistance is requested has a transnational character and, secondly, if the requested State is a party to the UNTOC.

When submitting the request based on the UNTOC, it is important to consult the online directory of competent national authorities or the printed version which will provide information about a central authority of the requested State, the channels of communication and other relevant information.<sup>174</sup> In order to ensure that the request is complete, it is highly recommended that the competent authority of the requested State make use of the UNODC Mutual Legal Assistance Request Writer Tool.<sup>175</sup> In case of an urgent request, it is vital to assess, based on the information available at the online directory, which exact communication channels need to be followed.<sup>176</sup>

### *United Nations Convention against Corruption (UNCAC), 2003*

The United Nations Convention against Corruption incorporates detailed and extensive provisions on international cooperation in criminal matters, including mutual legal assistance (Article 46). These provisions are generally based on the precedent of the UNTOC, sometimes going beyond it.

The UNCAC generally seeks ways to facilitate and enhance mutual legal assistance, encouraging States Parties to engage in the conclusion of further agreements or arrangements, improving the efficiency of mutual legal assistance. In any case, paragraph 1 of Article 46 requires States parties to afford one another the widest measure of mutual legal assistance as listed in Article 46(3) in investigations, prosecutions and judicial proceedings<sup>177</sup> in relation to the offences covered by the Convention. If the legal framework on mutual legal assistance of a State party is not broad enough to cover all the offences covered by the Convention, amending legislation may be necessary.

Article 46(2) mandates States parties to provide mutual legal assistance with respect to investigations, prosecutions and judicial proceedings in which a legal person is involved (see also Article 26 of the UNCAC).

#### *Types of mutual legal assistance allowed by the Convention*

Article 46(3) lists the types of assistance to be afforded under the UNCAC. In order to ensure compliance with this provision, States parties would need to conduct a thorough review of their legal framework on mutual legal assistance and assess whether such framework is broad enough to cover each form of cooperation listed in paragraph 3. States parties that have ratified the UNTOC would normally be

<sup>174</sup>The directory reveals the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific request of the receiving states and sometimes even extracts from the domestic legislation of that state.

<sup>175</sup>The software is available for downloading at: <http://www.unodc.org/mla/index.html>.

<sup>176</sup>A random example from the directory is the following: if country A needs to submit a MLA request to Belarus, the competent authority to receive such a request would be the General Prosecutor's Office in Minsk, the languages accepted are Belorussian and Russian, the request has to be transmitted through diplomatic channels but they accept the request to be anticipated through any means providing a written record as long as the originals will be sent via diplomatic channels and in urgent cases, they accept the transmittal through expedited means of communication with formal confirmation to follow.

<sup>177</sup>States parties have discretion in determining the extent to which they will provide assistance for such proceedings, but assistance should at least be available with respect to portions of the criminal process that in some States parties may not be a part of the actual trial, such as pretrial and sentencing proceedings, as well as release on bail.

in compliance with this provision and, in addition, they need to have appropriate mechanisms in place for providing assistance in cases of identifying, freezing and tracing proceeds of crime and asset recovery (see Article 46, paragraph 3(j) and (k)).

In the absence of an applicable mutual legal assistance treaty, the UNCAC provides a mechanism, pursuant to paragraphs 7 and 9-29 of Article 46, for the transmission and execution of requests with regard to the types of assistance mentioned above. If a treaty is in force between the States parties concerned, the rules of the treaty will apply instead, unless the State parties agree to apply paragraphs 9-29. In any case, States parties are also encouraged to apply those paragraphs to facilitate cooperation. In some jurisdictions, this may require additional legislation to give full effect to these provisions.

#### *Bank secrecy*

Article 46(8) provides that States parties cannot refuse mutual legal assistance on the ground of bank secrecy. It is significant that this paragraph is not included among the paragraphs that apply only in the absence of a mutual legal assistance treaty. Instead, States parties are obliged to ensure that no such ground for refusal may be invoked under their legal regime, including their Criminal Code, Criminal Procedure Code or the banking laws or regulations (see also Article 31(7), and Articles 55 and 57). Thus, where the legislation of a State party permits such a ground for refusal to be invoked, amending legislation will be required.

#### *Double criminality*

Paragraph 9 of Article 46 requires States parties to take into account the purposes and spirit of the UNCAC (Article 1) when they respond to requests for legal assistance in the absence of dual criminality. Although States parties may decline to render assistance in the absence of dual criminality (paragraph 9(b)), they are further encouraged to exercise their discretion and consider the adoption of measures that would broaden the scope of assistance even in the absence of this requirement (paragraph 9(c)).

However, to the extent consistent with the basic concepts of their legal system, States Parties are required to render assistance involving non-coercive action on the understanding that the assistance is not related to matters of a *de minimis* nature or cannot be provided under other provisions of the Convention (paragraph 9(b)).

#### *Designation of central authorities*

The Convention also requires the designation of a central authority (see paragraphs 13 and 14) with the power to receive and execute mutual legal assistance requests or transmit them to the competent domestic authorities for execution, thus providing an alternative to diplomatic channels. The judicial authorities of the requesting State can communicate with the central authority directly. Today, to an increasing degree, even more direct channels are being used, in that an official in the requesting State can send the request directly to an appropriate official in the other State.

#### *Spontaneous transmission of information*

Paragraphs 4 and 5 of Article 46 provide a legal basis for the spontaneous transmission of information, whereby a State party forwards to another State party information or evidence it believes is important to combat offences covered by the UNCAC at an early



stage where the other State party has not made a request for assistance and may be completely unaware of the existence of such information or evidence. The aim of these provisions is to encourage State parties to exchange information on criminal matters voluntarily and pro-actively. The receiving State party may subsequently use the information provided in order to submit a formal request for assistance. The only general obligation imposed for the receiving State party, which is similar to the restriction applied in cases where a request for assistance has been transmitted, is to keep the information transmitted confidential and to comply with any restrictions on its use, unless the information received is exculpatory to the accused person. In this case the receiving State party can freely disclose this information in its domestic proceedings.

*Differences from the UNTOC provisions*

Given that the UNTOC contains a similar provision on mutual legal assistance (Article 18), States parties to the UNTOC should, in general, be in a position to comply with the corresponding requirements arising from Article 46 of the UNCAC. Nevertheless, there are some significant differences between the two instruments.

Firstly, under the UNCAC, mutual legal assistance also extends to the recovery of assets, a fundamental principle of this Convention (see Articles 1 and 46(3)(j) and (k), as well as Chapter V of the Convention).

Secondly, in the absence of dual criminality, State parties are required to render assistance which does not involve coercive action, provided that it is consistent with their legal system and that the offence is not of a trivial nature. Such a provision was not incorporated to the UNTOC.

In addition, where dual criminality is required for the purposes of international cooperation in criminal matters, the UNCAC provides for an additional interpretation rule for the application of this rule which is not contained in UNTOC. It proposes that dual criminality criterion shall be deemed fulfilled irrespective of whether the laws of the requested State party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State party, if the activity or conduct, underlying the offence for which assistance is sought, is a criminal offence under the laws of both States parties (Article 43(2)). Furthermore, the Convention enables States parties not to limit themselves to cooperation in criminal matters, but also to assist each other in investigations of and proceedings in civil and administrative matters relating to corruption, where it is appropriate and consistent with their domestic legal system (Article 43(1)).

*Council of Europe Convention on Cybercrime, 2001*

The Convention contains several articles on mutual legal assistance, but the following chapter will only focus on Articles 25 and 27 of the Convention.<sup>178</sup> These articles refer to the general principles relating to mutual legal assistance and to the procedures pertaining to mutual legal assistance requests in the absence of applicable international agreements.

<sup>178</sup> For details, see Gercke, *Understanding Cybercrime...*, supra n. 26, page 207 et seq.

### *Conditions*

Article 23 of the Cybercrime Convention, entitled “General principles relating to international cooperation”, states that the chapter on international cooperation will apply in cases involving criminal offences related to computer systems and data, as well as for the collection of evidence of a criminal offence in electronic form. Although identity-related crime is not listed as a separate offence in the Convention on Cybercrime,<sup>179</sup> the provisions related to international cooperation are applicable.

Article 25(4) clearly mentions that the MLA requests shall be subject to the conditions provided for by the law of the requested party or by applicable mutual assistance treaties. This includes the grounds of refusal, thus providing a safeguard for the rights of the person located in the requested State, especially when dealing with intrusive measures.<sup>180</sup>

### *Types of MLA allowed and content of the request*

There are no special provisions dealing with the types of MLA and their content, but based on the general provisions, the types of MLA allowed under previous arrangements and their requirements with regard to the content of the request will remain applicable.

### *Channels and means of communication*

In the absence of international agreements that can be applied between the parties, the Convention requires the direct communication between the central authorities designated as such by States parties.<sup>181</sup> Still, in urgent cases, direct contact between the judicial authorities of the two cooperating States is possible. In any case, the Convention requires the transmission of a copy of the request to the central authority of the requested State as well. Another channel of communication that could be used in accordance with the Convention in case of urgent requests is the one offered by Interpol.

Article 27(9) enables States parties to make a declaration to the Secretary-General of the Council of Europe that they will continue to transmit urgent requests through the central authorities for reasons of better efficiency. However, a direct contact remains, from a practical point of view, the best way to deal with urgent requests, provided that the contact details of the other competent judicial authority are known to the requesting judicial authority.

With reference to the means of communications, the Convention<sup>182</sup> corresponds to the practical requirements concerning identity-related crimes by stipulating the use of expedited means of communication such as fax or e-mail with formal confirmation

<sup>179</sup> See, in this context, Gercke, Internet-related Identity Theft, Council of Europe Discussion Paper, 2007, available at: [http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd\\_meeting\\_docs/contributions/Internet\\_related\\_identity\\_theft\\_%20Marco\\_Gercke.pdf](http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf).

<sup>180</sup> See the Explanatory Report to the Convention on Cybercrime, paragraph 159, supra n. 159.

<sup>181</sup> Article 27(2)(a) and (b) recites the following:

(a) Each party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

(b) The central authorities shall communicate directly to each other.

<sup>182</sup> The article dealing with this is Article 25.

to follow if the requested state asks for such a measure. In such urgent cases, the response must be forwarded through the same means of communication.

#### *Spontaneous transmission of information*

The Convention permits the spontaneous transmission of information<sup>183</sup> to the receiving party without a prior MLA request in order to help this State initiate or carry out the investigations or criminal proceedings related to the offences stipulated by the Convention, or, if the issuing state believes that this could lead to a further request of cooperation from the receiving state. This regulation is similar to the relevant provisions of the UNTOC and the UNCAC, including the request of confidentiality with regard to sensitive information provided by the issuing state.

#### *Joint investigations*

The Convention does not make any specific reference to this form of cooperation. It does, however, refer to the relation of the Convention to other instruments. In view of this, it is possible that this form of cooperation will be allowed under other instruments applicable in certain cases and in consistency with relevant provisions of the domestic laws of the countries involved.

#### *Relationship with other instruments*

Article 39 defines the pre-eminence of other existing international agreements as the Convention does not affect the rights and undertakings derived from existing international multilateral conventions. The Convention also allows for the conclusion of bilateral agreements on matters dealt with in the Convention. However, where parties establish their relations in respect of the matters covered by the Convention through other agreements, they should do that in a manner that is not inconsistent with the objectives and principles of the Convention.

### *Inter-American Convention on Mutual Legal Assistance in Criminal Matters, 1992*<sup>184</sup>

Article 7 of the Convention, entitled “Scope of the application”, states that the assistance granted under the Convention will include the following procedures: the notification of documents; taking testimonies or statements; summoning of witnesses and expert witnesses to provide testimony; freezing of properties and assets and assistance in procedures related to seizures; searches or seizures, examination of objects and places; transmittal of documents, reports, information and evidence; transfer of sentenced persons; and finally “any other procedure provided there is an agreement between the requesting state and the requested state”. It should be noted that the scope of this Convention is wider than a similar regional Convention adopted at the European level, as it includes other issues of international cooperation in criminal matters which are dealt with in separate treaties in the European context (e.g. transfer of sentenced persons).

<sup>183</sup>Article 26 of the Convention on Cybercrime is relevant here. The Explanatory Report shows that the source of the such a provision reside in previous instruments adopted by the Council of Europe, namely Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, ETS No. 141, 1990 and Article 28 of the Criminal Law Convention on Corruption, ETS No. 173, 1999. See paragraph 260 of the Explanatory Report to the Convention, supra n. 157.

<sup>184</sup>The Convention is available at: <http://www.oas.org/juridico/english/treaties/a-55.html>. The status of ratification can be found on the same webpage.

### *Conditions*

In general, executing a request does not rely upon the double criminality requirement (Article 5(1) of the Convention), but there are also exceptions to this rule: if the request refers to the immobilization, sequestration, searches and seizures, house searches comprised, then the requested state *may* refuse to execute the MLA request (therefore the lack of double criminality requirement represents an optional ground of refusal). The grounds of refusal per se are mentioned in Article 9 and are optional as well (*ne bis in idem*, discrimination, political crime, requested issued at the request of a special or ad hoc tribunal, *ordre public*, sovereignty, security, and request referring to tax crimes).

The request will be executed in conformity with the law of the requested State and, to the extent possible, in the manner, specified by the requesting State, as long as the law of the requested State is not violated (Article 10 of the Convention).

### *Content of the request and other formal requirements*

The required content of the request is specified in Article 26 of the Convention, which refers to the offence for which assistance is requested, the summary of the relevant facts, the proceedings that give rise to the request and detailed description of the assistance sought.<sup>185</sup>

### *Channels of communication*

In accordance with Article 3 of the Convention, the transmittal and receipt of the requests shall be made through central authorities. Based on the best practices<sup>186</sup> elaborated during the Third Meeting of Central Authorities and Other Experts on Mutual Assistance in Criminal Matters and Extradition held in Bogota in 2007, a direct contact between the competent authorities of the requesting and requested States is encouraged before submitting the formal request.

### *Relationship with other instruments*

Article 36 of the Convention establishes the pre-eminence of other international, regional or bilateral instruments already in place, referring to any of the potential objects of request regulated by the Convention and to those instruments containing measures more favourable than those set forth in the Convention.

## *Optional Protocol Related to the Inter-American Convention on Mutual Assistance in Criminal Matters, 1993*

The Optional Protocol refers to tax crimes and provides modifications with regard to the practical application of Article 9(f) of the Convention pertaining to grounds of refusal, as well as Article 5 on double criminality. In this connection, a request for MLA assistance

<sup>185</sup>Article 26 of the Convention stipulates the following: “request for assistance shall contain the following details:  
(a) The crime to which the procedure refers; a summary description of the essential facts of the crime, investigation, or criminal proceeding in question; and a description of the facts to which the requests refers;  
(b) Proceeding giving rise to the request for assistance, with a precise description of such proceeding;  
(c) Where pertinent, a description of any proceeding or other special requirement of the requesting state;  
(d) A precise description of the assistance requested and any information necessary for the fulfilment of that request”.

<sup>186</sup>Proposed Best Practices with respect to the Gathering of Statements, Documents and Physical Evidence, with respect to the Mutual Legal Assistance in Relation to the Tracing, Restraint (Freezing) and Forfeiture (Confiscation) of Assets which are the Proceeds or Instrumentalities of Crime and Forms on Mutual Legal Assistance in Criminal Matters: adopted in Bogota, 12-14 September 2007, available at: [http://www.oas.org/juridico/MLA/en/model\\_law.pdf](http://www.oas.org/juridico/MLA/en/model_law.pdf).

cannot be refused solely on the ground that the offence is part of tax crimes. With regard to the double criminality, States parties to the Protocol, when acting as a requested State under the Convention, shall not decline assistance, if the act specified in the request corresponds to a tax crime of the same nature under the laws of the requested State.<sup>187</sup>

*Scheme Relating to Mutual Assistance in Criminal Matters within the Commonwealth (Harare Scheme), as last amended in 2005*<sup>188</sup>

The Scheme stipulates that the requested State has to inform the requesting State promptly if the request does not comply with the specific requirements of the Scheme and if there are grounds of refusal under the Scheme or reasons for delay,<sup>189</sup> while the execution of the request can be dependent upon the fulfilment of some conditions.<sup>190</sup> Apart from those conditions, there are established optional grounds of refusal. It is important to underline that under this Scheme the grounds of refusal are optional and not mandatory (Article 8). Among these grounds of refusal are the double criminality requirement, *ne bis in idem*, political or military offences, discrimination, *ordre public* and sovereignty.<sup>191</sup>

*Types of mutual legal assistance allowed*

The types of mutual legal assistance which can be requested under the Scheme<sup>192</sup> are the following: identifying and locating persons, service of documents; examining witnesses; search and seizure; obtaining evidence; temporary transfer of persons; obtaining judicial or official records; tracing, seizing and confiscating the proceeds or instrumentalities of crime and preserving computer data.

It should be emphasized that unlike other instruments, the Scheme also contains provisions related to preservation of computer data, which is a specific type of MLA, extremely relevant in identity-related crimes. In particular, Article 15 of the Scheme deals specifically with requests for the preservation of computer data. The preservation of computer data pursuant to a request made under this article shall be for a period of 120 (one hundred and twenty) days, pending submission by the requesting country of a request for assistance to obtain the preserved computer data. Following the receipt of such a request, the data shall continue to be preserved pending the determination of that request and, if the request is granted, until the data is obtained pursuant to the request for assistance. If the requested country considers that the preservation of computer data pursuant to a request made under this article will not ensure the future availability of the computer data, or will threaten the confidentiality of, or otherwise

<sup>187</sup> The text of the Optional Protocol can be found at: <http://www.oas.org/juridico/english/treaties/a-59.html> and the list of the states parties to the instrument at: <http://www.oas.org/juridico/english/Sigs/a-59.html>.

<sup>188</sup> The current form of the Harare MLA Scheme includes the changes brought in April 1990, November 2002 and October 2005, it applies to all 22 member States of the Commonwealth and can be found online at: [http://www.thecommonwealth.org/shared\\_asp\\_files/uploadedfiles/2C167ECF-0FDE-481B-B552-E9BA23857CE3\\_HARARESCHEME\\_RELATINGTOMUTUALASSISTANCE2005.pdf](http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/2C167ECF-0FDE-481B-B552-E9BA23857CE3_HARARESCHEME_RELATINGTOMUTUALASSISTANCE2005.pdf).

<sup>189</sup> See Article 7(3).

<sup>190</sup> See Article 7(4), which recites that “The requested country may make the granting of assistance subject to the requesting country giving an undertaking that:

- (a) The evidence provided will not be used directly or indirectly in relation to the investigation or prosecution of a specified person; or
- (b) A court in the requesting country will determine whether or not the material is subject to privilege”.

<sup>191</sup> See Article 8, Refusal of Assistance.

<sup>192</sup> See Article 1, Purpose and Scope, paragraph 3.

prejudice the investigation in the requesting country, it shall promptly inform the requesting country, which shall then determine whether the request should nevertheless be executed. Notwithstanding the general grounds for refusal contained in Article 8 of the Scheme, a request for the preservation of computer data under this article may be refused only to the extent that it appears to the requested country that compliance would be contrary to the laws and/or constitution of that country, or would prejudice the security, international relations, or other essential public interests of that country.

The fact that the Scheme attaches great importance to international cooperation with regard to cybercrimes in general, is reflected not only by the insertion of the above article, but also by the extensive space dedicated to definitions of terms such as subscriber information, computer system, computer data and traffic data.

#### *Content of the request and other formal requirements*

Reference to the required content of the MLA request is made in Article 14 (excluding preservation of data, mentioned in special provisions). The general requirements set forth in this article relate to the nature of the assistance sought, the time limit within which the request has to be fulfilled, the identification data of an agency or authority which issued the request, the nature of the criminal matter and to the fact whether criminal proceedings have been instituted. If the criminal proceedings have already been instituted, special requirements, provided thereto, shall apply. If no criminal proceedings have been instituted, the central authority of the requesting State has to specify the qualification of the offence which is reasonably believed to have been committed and to present a summary of the known facts. In urgent cases, the request can be made orally (with a subsequent written confirmation).

#### *Channels of communications*

According to Article 5 of the Scheme, requests shall be transmitted or received through central authorities. The Scheme clearly establishes the competences of the requesting and the requested States.<sup>193</sup>

#### *Relationship with other instruments*

As evident already in its introductory section,<sup>194</sup> the purpose of the Scheme is to enhance the “the level and scope of assistance rendered between Commonwealth Governments in criminal matters” and that, in this regard, it will not derogate from existing practices of cooperation, whether formal or informal.

### *Caribbean Treaty on Mutual Legal Assistance in Serious Criminal Matters, 2005*<sup>195</sup>

As the title indicates, this Treaty is applicable in cases of serious crimes (offences punishable by at least twelve months of imprisonment, including those offences related to taxation). The Treaty introduces a series of optional grounds for refusal, including *ordre public*, *ne bis in idem*, discrimination, political or military offences.<sup>196</sup> Double criminality or bank

<sup>193</sup> See Articles 6 and 7 of the Scheme.

<sup>194</sup> See paragraph 1 of Article 1, “Purpose and Scope”.

<sup>195</sup> The Treaty can be found online at: <http://www.caricomlaw.org/doc.php?id=554>.

<sup>196</sup> For details, see Article 7(1) of the Treaty.

secrecy does not constitute a pre-requirement for execution of the request.<sup>197</sup> There is a separate provision for each type of MLA allowed by the Convention, with more specific details which need to be followed when submitting a relevant request. Two of the articles are of importance for the purpose of this guide: Article 12 on “Service of Documents” and Article 13 on “Assistance in Gathering Evidence”.

#### *Types of mutual legal assistance allowed*

Article 2(3) stipulates that, as long as permitted by the law of the requested State, the following types of mutual legal assistance shall be undertaken on the basis of the Treaty: identifying and locating persons and objects; taking evidence or statements from persons; obtaining the production of judicial or other documents; effecting service of judicial documents; examining objects, sites and premises; providing information, originals or certified copies of any documents and records; facilitating the appearances of witness; effecting a temporary transfer of persons in custody; executing searches and seizures, tracing, freezing and confiscating the proceeds or instrumentalities of crime.

#### *Content of the request and other formal requirements*

In accordance with Article 5 of the Treaty, the request has to comprise the name of the competent authority, the purpose of the request, a description of the assistance sought, summary of the facts, legal provisions applicable, identification data of the person to be served (when speaking about service of documents), details about certain procedures to be followed by the requested state and the reasons why the requesting State is soliciting such information, as well as details about property to be traced or frozen, statement of the requesting state with regard to confidentiality and reasons for asking so from the requested State, and any other relevant information.

#### *Channels of communication*

Article 4 gives effect to the communication of MLA requests through central authorities having the responsibility and power to execute these requests or transmit them to the competent authorities for execution. Article 6 introduces an obligation for the requested State to act “as expeditiously as practicable” on requests for assistance.

#### *Relationship with other instruments*

Under Article 24, entitled “Other Arrangements”, it is stated that States parties may conclude other bilateral or multilateral treaty in order to supplement or strengthen the application of the CARICOM MLA Treaty.

### *ASEAN Treaty on Mutual Legal Assistance in Criminal Matters, 2004<sup>198</sup>*

The Treaty calls for the widest possible cooperation between States parties in the field of mutual legal assistance.<sup>199</sup> Nonetheless, limitations in granting the assistance,<sup>200</sup> include, among others, grounds for refusal related to political and military offences, discrimination

<sup>197</sup> See Article 7(3) and (4).

<sup>198</sup> The Treaty, signed in 2004 in Kuala Lumpur by the ASEAN member States, can be found online at: <http://www.aseansec.org/>.

<sup>199</sup> See Article 1(1) of the Treaty.

<sup>200</sup> See Article 3, *ibid.*

based on race, religion, sex, etc., *ne bis in idem*, double criminality, *ordre public*, sovereignty and failure to act on the basis of reciprocity.

#### *Types of mutual legal assistance allowed*

The purpose of the Treaty is clearly described in the very first article: facilitating a series of types of assistance, including taking of evidence; making arrangements for persons to give evidence or assist in criminal matters; effecting service of judicial documents; executing searches and seizures; examining objects and sites; providing originals or certified copies of documents; identifying and freezing of property; locating and identifying witnesses and suspects; and any other assistance that may be agreed in consistency with the Treaty and the legislation of the requested State.

#### *Content of the request and other formal requirements*

Article 6 of the Treaty comprises mandatory as well as optional requirements in relation to the content of the request.

Among the mandatory elements that should be present in the request are the following: the purpose of the request and the nature of the assistance sought; a statement with regard to the summary of the facts; a description of the facts and a copy of the legal texts applicable; a description of the evidence, information on assistance sought; indication whether a certain procedure or requirement needs to be followed and the reasons for doing so; a specification of the time limits (if any); and indication if confidentiality is required or any other information specifically required by the law of the requested state.

With respect to the optional requirements, depending on the type of the request, its content may contain, among others, the following: the nationality and location of the person or persons subject to investigations or from whom the evidence is sought or to whom the documents need to be served; information on the whereabouts of the person; the list of questions that need to be posed to a witness; a description of the property, asset or article to which the request relates; and a description of the manner in which a testimony or statement has to be taken and recorded.

#### *Channels of communication*

The Treaty establishes not only a direct contact between the central authorities, but also leaves the possibility of using the diplomatic channels open to the discretion of the States parties.<sup>201</sup> The provisions of the Treaty offer the possibility of using expedited means of communication when necessary and, as to the channels of communication, in urgent cases, transmission through Interpol or Aseanpol can also be possible.<sup>202</sup>

#### *Relationship with other instruments*

Article 23 of the Treaty accords priority to other treaties and arrangements on mutual legal assistance existing between States parties.

<sup>201</sup> See, in this sense, Article 4 of the Treaty.

<sup>202</sup> See Article 6 of the Treaty.



*SADC Protocol on Mutual Legal Assistance in Criminal Matters, 2002*<sup>203</sup>

The Protocol requires States parties to afford each other the widest possible assistance.<sup>204</sup> It is important to bear in mind that the double criminality principle is not a precondition for granting assistance: “Assistance shall be provided without regard to whether the conduct which is subject of investigation, prosecution or proceedings in the Requesting State would constitute an offence under the laws of the Requested State”. The request must be executed in accordance with the laws of the requested State and with the provisions of the Protocol.<sup>205</sup> An interesting provision is that of Article 4, which stipulates that the requested State should make all the necessary arrangements to allow the requesting State to be represented in any proceedings arising out of a request of assistance.

The Protocol stipulates in Article 6 some optional grounds of refusal. These refer to military and political offences, sovereignty, security and *ordre public*, as well as non-conformity with the provisions of the Protocol.

*Types of mutual legal assistance allowed*

Article 2 of the Protocol mentions among the types of assistance to be afforded under the Protocol those of locating or identifying persons, providing information and documents, service of documents, carrying out search and seizure, taking evidence and facilitating the appearance of witnesses.

*Content of the request and other formal requirements*

The content of the request is established in Article 5, which provides for both general and specific requirements, depending on the type of mutual legal assistance sought. The general requirements refer to the name of the competent authority in the requesting State, the nature of the investigation/proceedings, the summary of the facts, the provision of a copy of the legal provisions applicable, the identification of the purpose of the request, the nature of the assistance sought and the degree of confidentiality required.

*Channels of communication*

The Protocol requires that the central authorities are competent to make and receive mutual legal assistance requests and that they shall communicate directly to each other. Still, Article 3 provides for alternatives such as the use of diplomatic channels or Interpol.

*Relationship with other instruments*

Article 23, entitled “Relationship with other instruments”, stipulates that the provision of any treaty or bilateral agreements applied between any two of the States parties shall complement the Protocol and shall be applied in harmony with the provisions of the Protocol. In case of inconsistencies between the Protocol and the other instruments, the provisions of the Protocol shall prevail.

<sup>203</sup>The Protocol adopted by the Southern African Development Community can be found online at: <http://www.sadc.int/index/browse/page/156>.

<sup>204</sup>See Article 2 of the Protocol, Scope of application and obligation to provide MLA.

<sup>205</sup>See Article 4 of the Protocol.

*Council of Europe Convention on mutual assistance in criminal matters, 1959*<sup>206</sup>

*Conditions*

The Convention requires States parties to afford each other the widest measure of mutual assistance in proceedings in respect of offences the punishment of which falls within the jurisdiction of the judicial authorities of the requesting Party.<sup>207</sup> The optional grounds for refusal mentioned in Article 2 refer to political and fiscal offences (in the latter case, note the changes brought by the First Additional Protocol to the Convention), as well as sovereignty, *ordre public*, security or other essential interests of the requested Party. Concerning the letters rogatory, there are specific requirements mentioned in Article 5 of the Convention as follows:

- That the offence motivating the letters rogatory is punishable under both the law of the requesting Party and the law of the requested Party;
- That the offence motivating the letters rogatory is an extraditable offence in the requested country; and
- That execution of the letters rogatory is consistent with the law of the requested Party.

These are not mandatory grounds of refusal to execute the letters rogatory, but optional ones, allowing the parties to the Convention to submit a declaration in this respect.

*Types of mutual legal assistance allowed*

The Convention allows for various forms of cooperation, but bearing in mind the nature of the majority of requests for the purposes of this guide, letters rogatory and service of documents are the most relevant ones.

Letters rogatory are dealt with in Articles 3, 4 and 5 of the Convention. In general, the letters rogatory are to be executed in accordance with the law of the requested State. The Convention allows for the transmission of certified copies or photostat copies of the documents requested unless the requesting State expressly requests the transmission of originals.

Article 7 establishes as a main rule that the service of documents takes place through the simple transmission of the document to the person concerned. If it is requested that the service of documents need to take place in a certain manner provided by the law of requesting State, then the requested State shall act accordingly.<sup>208</sup> The proof of service shall be given by means of a receipt dated and signed by the person served or of a declaration made by the requested State confirming that the service has been effected and stating the form and date of such service.

<sup>206</sup>The decision to draw up a Convention on Mutual Legal Assistance in Criminal Matters was taken during the 41st Meeting of the Ministers' Deputies held in September 1956 when it was decided to instruct the experts to prepare a draft Convention on Mutual Assistance in Criminal Matters, see the Explanatory Report available at: <http://conventions.coe.int/Treaty/en/Reports/Html/030.htm>.

<sup>207</sup>See Article 1 of the Convention.

<sup>208</sup>See Article 7(1) of the Convention.

The service of documents to accused persons needs to be done with sufficient time prior to the actual term set for the trial. To that end, the Convention enables States parties to make declarations requesting that a service of a summons on an accused person be transmitted to its authorities by a certain time before the date set for appearance. This time should be specified in the declaration, but cannot exceed 50 days.<sup>209</sup>

*Content of the request and other formal requirements*

The general requirements regarding the content of the request are set forth in Article 14(1) and refer to the authority making the request, the object and reason of the request, the identity and nationality of the person concerned, if possible, the name and the address of the person to be served, when it concerns service of documents. Additional to that, there are specific requirements with regard to the letters rogatory. In such cases, the offence and the summary of the facts must be mentioned as well.

*Channels and means of communication*

The relevant provisions in this respect are included in Article 15 of the Convention. The contact between the Ministries of Justice of the requesting and requested States is the rule, and a direct contact between the judicial authorities can take place as far as the letter rogatory is concerned and only in case of urgency (nevertheless, the documents shall be returned through the central authorities). Another situation in which a direct contact is allowed is the one established through Article 13(1) of the Convention (on extracts and information relating to judicial records). When a direct transmission is allowed, it may take place even through Interpol (this provision has been slightly changed by the Second Additional Protocol).

Another important aspect to be underlined is that the Convention confers pre-eminence to other bilateral agreements or arrangements, allowing a direct transmission of MLA requests, in force between the parties.<sup>210</sup>

*Relationship with other instruments*

This subject is dealt with in Article 26 of the Convention. According to the first paragraph, the 1959 Convention will supersede other treaties, conventions or bilateral agreements governing MLA between the parties, with the exception of the provisions related to the direct transmission of requests and translation of the requests and annexed documents, which will remain governed by the former treaties, arrangements, etc.<sup>211</sup>

The Convention does not, however, affect the specific obligations concerning mutual legal assistance in a given field through previous bilateral or multilateral instruments.

As for the future bilateral or multilateral agreements, they can be concluded in order to supplement the provisions of the Convention or to facilitate their application.

<sup>209</sup> See Article 7(3), *ibid.*

<sup>210</sup> See Article 15(7), *ibid.*

<sup>211</sup> See Article 26(1) of the Convention as well as the Explanatory Report available at: <http://conventions.coe.int/Treaty/en/Reports/Html/030.htm>.

### *First Additional Protocol of 1978 to the Convention of 1959*<sup>212</sup>

The first Additional Protocol includes norms introducing amendments of the text of the Convention with regard to fiscal offences, service of documents concerning the enforcement of a sentence, recovery of a fine (see Article 3 of the Protocol), as well as changes to Article 22 of the Convention on the exchange of information from judicial records (see Article 4 of the Protocol).

It is important to mention that the Protocol confers pre-eminence to “more extensive regulations in bilateral and multilateral arrangements concluded between Contracting Parties” in application of Article 26(3) of the Convention (which allows States parties to conclude other arrangements or instruments in order to supplement the provisions of the Convention or to facilitate the application of these provisions).

### *Second Additional Protocol of 2001 to the Convention of 1959*<sup>213</sup>

More relevant for the purpose of this guide is the Second Additional Protocol 2001, which has introduced changes with regard to the channels of communication (Article 4 of the Protocol), as well as new forms of cooperation. These include hearing by videoconference or by telephone conference, cross-border observations, controlled delivery and covert investigations, as well as joint investigation teams. Many of these provisions are also found in the EU Convention 2000 (see below). Due to space restrictions, but also in light of a general orientation of this guide, reference shall be made only to some of the provisions of the Protocol, namely to those referring to the channels of communication, spontaneous transmission of information and joint investigation teams.

#### *Channels of communication*

Article 4 establishes as a general rule that requests are channelled through the Ministries of Justice of the cooperating States. Article 4 also maintains the possibility of a direct contact between the judicial authorities of the requesting and requested States. The same direct contact can be applied with regard to controlled deliveries and covert investigations, as well as letters rogatory in general, although there are some MLA requests that will continue to be transmitted and received through central authorities (e.g. requests on temporary transfer of witnesses or detained persons to the requested state). Direct contact can also be possible with reference to the transmittal of copies of convictions and information related to judicial records.<sup>214</sup>

In case of urgency, Interpol can be used. It should be emphasized that Article 4(7) of the Second Additional Protocol reduces the possibilities to use the Interpol channels only to urgent cases, while the Convention, in Article 15(5), allows for such transmission in general, when direct contact is permitted.

<sup>212</sup>The text of the Additional Protocol and the Explanatory Report can be found at: [http://www.asser.nl/default.aspx?site\\_id=8&level1=10785&level2=10861](http://www.asser.nl/default.aspx?site_id=8&level1=10785&level2=10861).

<sup>213</sup>The text of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS No. 182, available at: <http://conventions.coe.int/treaty/en/Treaties/word/182.doc>.

<sup>214</sup>See Article 4(5) and (6) of the Second Additional Protocol, *ibid*.

The Protocol leaves it open for States parties to transmit copies of the request to the central authorities even in urgent cases or to send some of the requests through other channels (diplomatic channels included).

It should be highlighted that Article 16 enables a State party to effect the service of procedural and judicial documents directly by posting them to the persons located on the territory of another State party.<sup>215</sup> The same article also brings innovations with respect to the means of communication, which are extremely important when dealing with volatile data such as in computer cases or identity-related cases in general. Paragraph 9 of Article 4 specifies that the requests may be forwarded by using electronic or other means of communication, as long as a written record is also produced.

#### *Spontaneous transmission of information*

Article 11 of the Protocol allows for the competent authorities of one party to forward to the competent authorities of another party the information obtained in course of their own investigation, when they believe that such information could help the receiving country in initiating or carrying on its investigations.<sup>216</sup>

#### *Joint investigation teams*

Article 20 of the Protocol establishes the basis for creating JITs among the Council of Europe Member States and is very similar to Article 13 of the EU 2000 Convention on Mutual Assistance in Criminal Matters.

### *Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000<sup>217</sup>*

Pursuant to this Convention, mutual legal assistance is to be afforded in accordance with the requirements of the requesting State unless the formalities and procedures would contravene the principles of the domestic law in the requested State. This provision departs from the traditional practice whereby the request has to be executed in accordance with the domestic provisions of the requested State.

#### *Types of mutual legal assistance allowed*

The Convention supplements the so-called parent conventions in this field, including the Council of Europe 1959 Convention and the 1978 Additional Protocol to this Convention, as well as the provisions on MLA of the 1990 Schengen Agreement. Under the 2000 Convention, specific forms of mutual assistance are regulated, such as videoconference (Article 10), telephone conference (Article 11), controlled deliveries (Article 12), joint investigation teams (Article 13), and covert investigations (Article 14). There are also important provisions related to the interception of telecommunication (Articles 17-22). For the purpose of this guide, special reference shall be made to Articles 5, 6, 7 and 13.

<sup>215</sup> For details, see Article 16, *idem*.

<sup>216</sup> See Article 11, *idem*, as well as the Explanatory Report to the Second Additional Protocol, available at: <http://conventions.coe.int/treaty/en/Reports/Html/182.htm>.

<sup>217</sup> The text of the Convention, of the Additional Protocol as well as the Explanatory Reports can be found at: [http://ec.europa.eu/justice\\_home/doc\\_centre/criminal/acquis/doc\\_criminal\\_acquis\\_en.htm](http://ec.europa.eu/justice_home/doc_centre/criminal/acquis/doc_criminal_acquis_en.htm).

*Content of the request*

On this issue, the general requirements set forth in the parent conventions will be applicable.

*Channels and means of communication*

The requests shall be made in writing, by any means capable of reproducing a written record. Article 6(1) of the Convention establishes a direct contact between the issuing and executing judicial authorities as a rule. However, this requirement does not impede the transmittal between central authorities or between a judicial authority of one State party and the central authority of another State party. There are some types of requests (e.g. temporary transfers of persons held in custody) which should still be made through central authorities in all cases.<sup>218</sup>

With regard to the service of procedural documents, the Convention is again quite innovative in comparison to the previous instruments (provisions which will be taken over also by the Second Additional Protocol to the 1959 MLA Convention of the Council of Europe), establishing, as a general rule, the transmittal of documents directly by post to the intended recipient in the other EU Member State.

Procedural documents may be sent via the competent authorities of the requested Member State only if:

- The address of the person for whom the document is intended is unknown or uncertain; or
- The relevant procedural law of the requesting Member State requires proof of service of the document on the addressee, other than proof that can be obtained by post; or
- It has not been possible to serve the document by post; or
- The requesting Member State has justified reasons for considering that dispatch by post will be ineffective or is inappropriate.<sup>219</sup>

*Spontaneous exchange of information*

Article 17 enables States parties, within the limits of their national laws, to exchange without a prior request information relating to criminal offences or infringements of the rules of law which would have to be dealt with by the receiving authorities.

*Joint investigation teams*

As previously mentioned, the JIT concept is becoming more and more important since the phenomenon of transnational criminality has expanded. Due to the slow process of ratification of the Convention, the same provisions were taken over in a Council Framework Decision on Joint Investigation Teams adopted on 13 June 2002, which should have been implemented by the Member States by 2003.<sup>220</sup>

<sup>218</sup> See Article 6(8) of the Convention.

<sup>219</sup> See Article 5(2)(a) to (d), *ibid.*

<sup>220</sup> For details, see the Joint Investigation Teams Manual adopted by Europol and Eurojust as well as Implementation of the European Arrest Warrant and Joint Investigation Teams at the EU and National Level (Study), January 2009, released by the Directorate General Internal Policies, Policy Department C, Citizens' Right and Constitutional Affairs, available at: [http://www.ecba.org/cms/index.php?option=com\\_content&task=view&id=259&Itemid=21](http://www.ecba.org/cms/index.php?option=com_content&task=view&id=259&Itemid=21).

The JIT can be established for a specific purpose and for a limited period of time in order to carry out investigations in one or more of the Member States which set up the team. This is done through means of a mutual agreement.<sup>221</sup>

Setting up a JIT can occur when the investigations in one Member State prove difficult and are dependent on subsequent investigations in other Member States, or when a number of Member States are conducting investigations that need coordinated and concerted actions. A joint investigation team operates in the territory of the Member State setting up the team, under the condition that the operations are conducted in accordance with the law of the State where it operates and the leader of the team will be from that State.

As for the members of the team, other than those coming from the state where the team operates, they are called seconded members. Their competence and their use of information obtained during investigation are clearly established under Article 13, paragraphs 5 to 10, of the Convention.

#### *Relationship with other instruments*

Unlike other instruments that insert the relevant articles in the end, the EU 2000 Convention establishes these aspects from the very beginning under Article 1 (Relationship to other conventions on mutual assistance) by stipulating that the EU 2000 Convention will supplement and facilitate the application of the provisions of the Council of Europe 1959 Convention on Mutual Legal Assistance in Criminal Matters and its Additional Protocol of 1978, as well as those of the Schengen Convention of 19 June 1990, and Chapter 2 of the Benelux Treaty. Due to these provisions, it is considered that the Convention cannot be invoked when formulating a MLA request alone, but always in conjunction with the parent Convention it supplements. In case of contradictory provisions between the two, the EU 2000 Convention will prevail.<sup>222</sup>

### *Protocol 2001 to the Convention of 2000*

The Protocol is mainly relevant for the provisions referring to information on bank accounts and bank transactions, which could be useful in the context of the identity-related crime and its connection with money laundering.<sup>223</sup>

### *Conclusions*

Despite the fact that all these instruments have been adopted under different regional contexts and reflect many differences, there are several elements that appear recurrent. As an issuing judicial authority or executing judicial authority, it is crucial to follow some

<sup>221</sup> A form of a model agreement for setting up a JIT was proposed through the Council Recommendation of 8 May 2003 on a model agreement for setting up a Joint Investigation Team. Currently the matter is under discussion at EU level on its updated version.

<sup>222</sup> See the Explanatory Report to the Convention, available online at: [http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229\(02\)&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229(02)&model=guichett).

<sup>223</sup> For the interpretation of its provisions, see the Explanatory Report available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2002:257:0001:0009:EN:PDF>.

essential steps in order to optimize the cooperation in identity-related crime cases, based on the existing instruments.

Before submitting the formal request, some initial and valuable inputs can be offered by means of police or law enforcement cooperation. Previous consultations with the executing state can also prove very useful.

For the majority of instances, communication of the documents takes place through central authorities and situations of transmittal through diplomatic channels are not excluded. This is a very time-consuming procedure and the requesting or requested judicial authority has to find the best solution in order to get a prompt response. In the majority of cases, that would mean a direct contact or, if the treaty in force does not allow this, the use of available networks, where personal contacts between the contact points are extremely important (an aspect which will be tackled later on, in the end of the present chapter). Quite often, responses in a short period of time depend on how complete the request was and if it followed the procedures specified in the applicable Treaty or the special requirements of the domestic law of the executing state.

In identity-related crimes, one has to deal with problems and challenges of a transnational nature.<sup>224</sup> As it will be shown in the case studies section, this would entail, on many occasions, the involvement of multiple jurisdictions and various legal systems. In these situations, coordination becomes essential in order to get the desired results. Use of JITs can be one of the best solutions to be adopted under these circumstances.

Establishing good practices<sup>225</sup> in the field and submitting the person in charge of MLA requests to continuous training are other aspects that need to be taken into account, in order to improve results in daily casework. Continuous dialogue, use of the tools and training provided for by the international organizations are among the key factors for achieving enhanced cooperation with regard to this type of criminality.

#### 4. Specific forms of mutual legal assistance provided through the Council of Europe Convention on Cybercrime and the Harare MLA Scheme which can be relevant in identity-related crime

As previously stated, the Cybercrime Convention of the Council of Europe has introduced some specific forms of mutual assistance,<sup>226</sup> which were designed to pay attention to the specificity of cybercrime and crimes committed by using the Internet as a means. It is important to know that States parties to the Convention do have such provisions in their

<sup>224</sup>Details about international cooperation in identity-related crimes can be found also in: International Cooperation in the Prevention, Investigation, Prosecution and Punishment of Economic Fraud and Identity-Related Crime, Report of the Secretary-General, E/CN.15/2009/2, Vienna, 16-24 April 2009.

<sup>225</sup>See the Report of the Informal Expert Working Group on Mutual Legal Assistance Casework Best Practice, available at: [http://www.unodc.org/pdf/lap\\_mlaeg\\_report\\_final.pdf](http://www.unodc.org/pdf/lap_mlaeg_report_final.pdf), which contains in its final part also model checklists and forms.

<sup>226</sup>For a detailed analysis of mutual legal assistance focused on provisional measures under the Council of Europe Cybercrime Convention, see Cybercrime Training for Judges (Training Manual), version 4, March 2009, prepared by Gercke, page 84 et seq., available at: <http://www.coe.int/cybercrime>.



national laws. Other countries, although they have not signed or ratified the Convention, may have introduced such measures in their domestic legislation. Apart from that, special reference will be made also to the article on data preservation and the article present in the Harare MLA Scheme, which was briefly mentioned in the pages referring to the Commonwealth instrument.<sup>227</sup>

Articles 29–33 of the Convention on Cybercrime represent the “MLA equivalent” to the corpus of provisions establishing specific procedural instruments,<sup>228</sup> which are designed to streamline cybercrime investigations in States parties.<sup>229</sup> With regard to the principle of national sovereignty, these instruments can only be used for investigations at the national level.<sup>230</sup> If the investigators realize that evidence needs to be collected outside their territory, they need to request for mutual legal assistance. Each of the instruments established by Articles 16–21 has a corresponding provision in Articles 29–33, thus enabling the law enforcement agencies to apply the procedural instruments on a request of a foreign law enforcement agency.

*Expedited preservation of stored computer data—Article 29 of the Council of Europe Cybercrime Convention*

This provision is very important for the investigation of both cybercrime, in general, and identity-related crime, in particular. It allows the requesting State to ask the requested State to preserve stored data, gaining therefore extra time before actually submitting the formal MLA request. The latter would consist in search, seizure or disclosure of the data. This is quite a logical measure, taking into account the volatility of data in cyberspace, as it impedes the deletion, alteration or removal of the data by the offender. Article 29 provides for a mechanism at the international level equivalent to that provided for in Article 16 for use at the domestic level.<sup>231</sup> The content of the request for preservation is stipulated in Article 29(2), specifying the authority that seeks the preservation, as well as the offence subject of the investigation, the summary of the facts, the stored computer data that need to be preserved, information about the custodian of the stored computer data, the necessity of preservation and the mentioning of the fact that the issuing authority will submit a MLA request further on.<sup>232</sup> Double criminality constitutes a ground of refusal only if the offence under discussion is other than those stipulated in Articles 2–11 of the Cybercrime Convention and even so, it represents an optional ground of refusal. Other optional grounds of refusal are sovereignty and *ordre public*, as well as political offences.<sup>233</sup> The data can be preserved for a term of at least 60 days, pending receipt of a formal mutual legal assistance request.

<sup>227</sup> See *supra*, under section 3.6.

<sup>228</sup> See *Gercke*, *Understanding Cybercrime...*, *supra* n. 26, chapter 6.2.

<sup>229</sup> The most important procedural instruments established by the Convention on Cybercrime are: Expedited preservation of stored computer data (Article 16), Expedited preservation and partial disclosure of traffic data (Article 17), Production order (Article 18), Search and seizure of stored computer data (Article 19), Real-time collection of traffic data (Article 20), Interception of content data (Article 21).

<sup>230</sup> An exception is Article 32 Convention on Cybercrime. Regarding the concerns related to this instrument see: Report of the second Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: “[...] Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32(b) in particular in the light of experience gained from the use of this article).”

<sup>231</sup> See the Explanatory Report to the Council of Europe Cybercrime Convention, *supra* n. 157, paragraph 282.

<sup>232</sup> For a proposed checklist for requests for expedited preservation see The functioning of the 24/7 points of contact for cybercrime, the Discussion paper, available at: <http://www.coe.int>, and the G8 data preservation checklist available at: [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Data%20PreservationChecklists\\_en.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Data%20PreservationChecklists_en.pdf).

<sup>233</sup> See Article 29(5).

*Requests for the preservation of computer data under the Harare MLA Scheme*

In general, the data preservation request under this instrument does not differ in terms of content with the requirements mentioned in the Council of Europe Cybercrime Convention.<sup>234</sup> The main difference is the time limit, which in this case is 120 days. The refusal to execute such a request could appear only if “it appears to the requested country that compliance would be contrary to the laws and/or constitution of that country or would prejudice the security, international relations, or other essential public interest of that country”.

*Expedited disclosure of preserved traffic data—Article 30 of the Council of Europe Cybercrime Convention*

Article 30 provides the international equivalent of the power established for domestic use in Article 17. Frequently, at the request of a party in which a crime was committed, a requested party will preserve traffic data regarding a transmission that has travelled through its computers, in order to trace the transmission to its source and identify the perpetrator of the crime, or locate critical evidence. In doing so, the requested party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself. In such cases, the requested party must expeditiously provide to the requesting party a sufficient amount of the traffic data to enable identification of the service provider in, and path of the communication from, the other State. If the transmission came from a third State, this information will enable the requesting party to make a request for preservation and expedited mutual assistance to that other State in order to trace the transmission to its ultimate source. If the transmission had looped back to the requesting party, it will be able to obtain preservation and disclosure of further traffic data through domestic processes.<sup>235</sup>

The requested party may only refuse to disclose the traffic data, where disclosure is likely to prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. As in Article 29 (Expedited preservation of stored computer data), because this type of information is so crucial to identification of those who have committed crimes within the scope of this Convention or locating of critical evidence, grounds for refusal are to be strictly limited, and it was agreed that the assertion of any other basis for refusing assistance is precluded.

*Mutual legal assistance regarding accessing of stored computer data—Article 31 of the Council of Europe Cybercrime Convention*

Once again, this article corresponds to a similar measure disposed at internal level, as stipulated by Article 19 of the Convention, “Search and seizure of stored computer data”. The requested State has to execute the request in accordance with the international instruments and arrangements already existing between it and the requesting State (in this sense, special reference is made to Article 23 of the Convention) and if necessary, in an expedited manner.<sup>236</sup>

<sup>234</sup> See Article 15(2) of the Scheme.

<sup>235</sup> See for details with regard to the interpretation of this article the Explanatory Report, supra n. 157, paragraphs 290 and 291.

<sup>236</sup> See Article 31(3)(a) and (b).

*Mutual assistance in the real-time collection of content data—Article 33 of the Council of Europe Cybercrime Convention*

The article establishes the basis of the international cooperation in the real-time collection of traffic data, giving pre-eminence to existing treaties and arrangements allowing for this type of cooperation.<sup>237</sup>

*Mutual legal assistance regarding the interception of content data—Article 34 of the Council of Europe Cybercrime Convention*

Because of the high degree of intrusiveness of interception, the obligation to provide mutual legal assistance for interception of content data is restricted. The assistance is to be provided to the extent permitted by applicable treaties and domestic laws of the States parties. As the provision of cooperation for interception of content is an emerging area of mutual legal assistance practice, it was decided to defer to existing mutual legal assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist.<sup>238</sup>

## 5. The role of networking in solving the MLA requests

Having access to different networks and institutions that facilitate networking is one of the fundamental issues in getting prompt and fast responses. There are different regional networks which can prove their functionality at the regional level, as well as institutions which work at the bilateral level, such as the liaison magistrates. In the era of globalization, the need for regional networks to work together as a global network is felt more than ever. The presentation of the legal framework on international cooperation in the identity-related crime cases cannot ignore this aspect, as, on many occasions, the use of regional networks achieves faster and more successful results. Although these networks are mainly informal, the contact points can offer valuable information about legal systems and contact details of competent authorities, thus facilitating the transmittal of mutual legal assistance requests.

### *The 24/7 networks*

There are several operational 24/7 networks, including the network designed under the G8 framework and the network developed by the States parties to the Council of Europe Cybercrime Convention. The task of a 24/7 network is to assure around-the-clock availability of the contact points, so that the provisional measures which need to be taken with regard to cybercrime (including forms of identity-related crime committed online) can be disposed as soon as possible.

Cybercrime investigations often require immediate reaction.<sup>239</sup> To increase the speed of international investigations, the European Convention on Cybercrime highlights the

<sup>237</sup> See the Explanatory Report, supra n. 157, paragraphs 295 and 296.

<sup>238</sup> See the Explanatory Report, ibid, paragraph 297.

<sup>239</sup> The need to speed up the process of international cooperation is pointed out in the Explanatory Report: “Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to.”

importance of enabling the use of expedited means of communication in Article 25. In order to further improve the efficiency of mutual assistance requests, the Convention requires that States parties designate contact points for the mutual legal assistance requests and that these contact points be available without time limitations.<sup>240</sup> The drafters of the Convention emphasized that the establishment of the points of contact is one of the most important measures provided for by this instrument.<sup>241</sup>

According to Article 35 of the Cybercrime Convention, the contact points are entrusted with the task to offer technical advice, preserve data pursuant to Articles 29 and 30 of the Convention, collect evidence, locate suspects or provide legal information. The States parties have made declarations to identify their domestic bodies in charge of those tasks. A list of the contact points can be found on the Council of Europe website.<sup>242</sup> Other important elements are highlighted in the discussion paper “The functioning of 24/7 points of contact for cybercrime”, available on the same website.

### *European Judicial Network (EJN) and EUROJUST within EU*

#### EJN

The European Judicial Network was established in 1998 by Joint Action 98/428/JHA and comprises contact points among the central authorities and judicial authorities of the Member States and the European Commission. The current instrument dealing with the European Judicial Network dates from 2008.<sup>243</sup> According to Article 4 of the Joint Action, the contact points function as active intermediaries with the task of facilitating judicial cooperation between the Member States, particularly in action to combat serious crime (organized crime, corruption, drug trafficking and terrorism). They also provide the necessary legal and practical information to the local judicial authorities in their own countries, as well as to the contact points and local judicial authorities in other countries, in order to enable them to prepare an effective request for judicial cooperation or improve judicial cooperation in general. Furthermore, their task is to improve coordination of judicial cooperation in cases where a series of requests from the judicial authorities of a Member State necessitates coordinated action in another Member State.

The contact points have access to a secure telecommunication system. The European Judicial Network has a list of resources password protected, but some materials, forms and information are also available on the public website.<sup>244</sup> The same public component comprises also the European Judicial Atlas in relation to the European arrest warrant and mutual legal assistance.

<sup>240</sup>The availability 24 hours a day and 7 days a week is especially important with regard to international dimension of Cybercrime as requests can potentially come from any time zone in the world. Regarding the international dimension of Cybercrime and the related challenges, see *Gercke, Understanding Cybercrime...*, supra n. 27, chapter 3.2.6.

<sup>241</sup>See Explanatory Report, supra n. 157.

<sup>242</sup>The list can be found at: [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/International\\_cooperation/Res\\_internatcoop\\_authorities\\_en.asp](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/International_cooperation/Res_internatcoop_authorities_en.asp).

<sup>243</sup>Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network.

<sup>244</sup>In this respect, see: <http://www.ejn-crimjust.europa.eu/>.

## EUROJUST

Eurojust is a body consisting of 27 National Members, located in the Hague. It was founded in 2002 by a European Council Decision,<sup>245</sup> amended in 2003 and 2009. Eurojust aims at stimulating and improving coordination of investigations and prosecutions in the Member States, improving cooperation between the competent authorities of the Member States, in particular by facilitating the execution of international mutual legal assistance and the implementation of extradition requests, as well as supporting otherwise the competent authorities of the Member States in order to render their investigations and prosecutions more effective (Article 3 of the Council Decision). It consists of a national member appointed by each Member State in his/her capacity as a prosecutor, judge or police officer of equivalent competences (Article 2 of the Council Decision).

Eurojust can conclude agreements with third countries and international organizations. A report on the activity of the cooperation body is released annually and the latest reports indicate that identity-related crimes are among the crimes tackled by this body in an efficient manner.<sup>246</sup>

### *PC-OC point of contacts*

This is a network of experts developed in the framework of the Committee of Experts on the Operation of European Conventions on Cooperation in Criminal Matters (PC-OC)<sup>247</sup> and is constituted from contact points of the Council of Europe Member States. They have access to a restricted website and their work is no different from that undertaken by the EJM contact points. On many occasions, the same person holds the position of contact point in the EJM and as the PC-OC.

### *The Commonwealth Network of Contact Persons (CNCP)*

This network was established in 2007 and comprises representatives from 53 Member States, originating from various regions (it allows the presence of Member States in other regional networks). The purpose of establishing such an informal network was to facilitate international judicial cooperation in criminal matters with regard to extradition and mutual legal assistance and to offer legal and practical advice on the application of the main instruments in the field.<sup>248</sup> Access to this informal network is password protected and made through a secure website.

<sup>245</sup> See the Council Decision 2002/187/JHA of 28 February 2002, setting up Eurojust with a view to reinforcing the fight against serious crime (the consolidated version resulted from the amendments brought by Decision 2003/659/JHA and Decision 2009/426/JHA).

<sup>246</sup> The Annual Reports as well as other relevant materials can be found at: <http://www.eurojust.europa.eu/>.

<sup>247</sup> For details and legal information with regard to Member States on various topics, extradition and mutual legal assistance being comprised, see: [http://www.coe.int/t/e/legal\\_affairs/legal\\_co-operation/Transnational\\_criminal\\_justice/](http://www.coe.int/t/e/legal_affairs/legal_co-operation/Transnational_criminal_justice/).

<sup>248</sup> For more details see the Framework of the CNCP, available at: [http://www.thecommonwealth.org/shared\\_asp\\_files/uploadedfiles/1D0DC9F4-815A-4B0E-8B9D-718209E46D77\\_COMMONWEALTHNETWORKOFCONTACTPERSONS\(CNCP\).pdf](http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/1D0DC9F4-815A-4B0E-8B9D-718209E46D77_COMMONWEALTHNETWORKOFCONTACTPERSONS(CNCP).pdf)

*The Ibero-American Legal Assistance Network (Red Iberoamericana de Cooperación Jurídica Internacional)—IberRed*

IberRed is a network formed in 2004<sup>249</sup> that currently comprises 21 States from Latin America and 2 European States—Spain and Portugal. It has contact points established between the central authorities of Member States and the access to this list of contact points is password protected. On the other hand, the website of the regional network also has a public component, providing information about the domestic legislation of each of its countries.<sup>250</sup>

Currently a Memorandum of Understanding has been developed between IberRed and the European Judicial Network,<sup>251</sup> which can be considered an important step towards facilitating future requests for assistance.

*The Hemispheric Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition of the Organization of American States*<sup>252</sup>

This network is a regional network developed by the Organization of American States (OAS) started in 2000, as a consequence of the decision taken at the Third Meeting of the Ministers of Justice or of Ministers or Attorneys Generals of the Americas (REMJAS). The declared aim of this network is to improve the mutual cooperation between Member States. To that end, the network was designed on the basis of a three-level component: a public one (primarily an online library comprising information about the law system of every Member State); a private website with contact details of representatives from each country; and a secure electronic communication system comprising an online forum for discussions.

*UNODC online directory of Competent National Authorities*<sup>253</sup>

The UNODC on line Directory of Competent National Authorities allows easy access to the contact information of competent national authorities designated under the 1988 Drugs Convention and the United Nations Convention against Transnational Organized Crime and the Protocols thereto. The directory contains the contact information of over 600 CNA's authorized to receive, respond to and process requests for extradition, transfer of sentenced persons, mutual legal assistance, illegal traffic of narcotics by sea, smuggling of migrants by sea and trafficking in firearms.

With the view to facilitate communication and problem-solving among competent authorities at the interregional level, the Directory contains essential information on:

- State membership in existing regional networks;
- Legal and procedural requirements for granting of requests;

<sup>249</sup> For details see: <http://www.iberred.org/presentacion/>.

<sup>250</sup> Available at: <http://www.iberred.org/legislaciones/>.

<sup>251</sup> The Memorandum is available at: <http://www.iberred.org/assets/Uploads/Memorandum-de-Entendimiento-IberRed-Eurojust.pdf>.

<sup>252</sup> For more details about the history of the network, see: <http://www.oas.org/juridico/MLA/en/index.html>.

<sup>253</sup> See: <http://www.unodc.org/compauth/en/index.html>.

- Use of the UNTOC as the legal basis for requests;
- Links to national laws and websites; and
- Indication of requests that can be made through Interpol.

The on line directory is available to competent authorities and government agencies with a user account. Account members also receive the latest publication of the Directory twice a year and can download the directory in .pdf and .rtf formats.

### *Liaison magistrates*

The role of liaison officers in law enforcement cooperation was mentioned earlier. In this context, it should be highlighted that liaison magistrates play an equally important role in mutual assistance in criminal matters. The liaison magistrates usually facilitate contact between the central authorities involved or the direct contact between the judicial authorities of the two countries involved. The liaison magistrates directly participate in the transmittal of rogatory letters and any other mutual legal assistance requests, including those referring to identity fraud. They can also participate in exchanging information about the legal systems and statistical data. They can further intervene in cases of extraditions, as an intermediary in case the requested State asks for supplementary information, but they can also facilitate other requests preceding the extradition per se. Normally the liaison magistrates are exchanged between countries based on bilateral agreements. At European level, the reference instrument is represented by the Council Joint Action 96/277/JHA of 22 April 1996 concerning a framework for the exchange of liaison magistrates to improve judicial cooperation between the Member States of the European Union.<sup>254</sup>

<sup>254</sup> For more details, see: [http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996F0277&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996F0277&model=guichett).







## V. CASES

This chapter provides an overview about typical identity-related crime cases. Following the aim of the Guide to provide a first access to the subject matter, especially for those experts who are investigating such offences, each case provides strategy information and practical guidance.

### 1. First case—cloned credit cards

*Focus of the case:* Rogatory letter during the trial phase. Use of cloned credit cards.

#### *Facts of the case*

One citizen of country A uses cloned credit cards in country B. Both countries belong to the European Union. The above-mentioned citizen is currently under the trial procedure in country B.

#### *Background information*

Credit card cloning describes the act of duplicating an existing credit card.<sup>255</sup> This can, for example, be done by using devices that read the information on the magnetic stripe and then write that information on a blanket magnetic card.<sup>256</sup> Very often the credit card information is obtained from legitimate payment processes—for example when the victim pays with a credit card at a petrol station or restaurant.<sup>257</sup> Very often credit card cloning is a follow up to skimming. The term “skimming” is in general used to describe an offence where the offenders manipulate an ATM in order to obtain credit card information and personal identification numbers.<sup>258</sup> Credit card information obtained by manipulating ATMs<sup>259</sup> is then used to clone the original cards and use them from crimi-

<sup>255</sup> Regarding the phenomenon of cloning in relation to identity-related crime, see *Wall*, *Cybercrime: The Transformation of Crime in the Information Age (Crime and Society)*, Polity Press, 2007, page 80.

<sup>256</sup> *Greene*, *Encyclopedia of Police Science*, Routledge, 2006, 2nd edition, page 646.

<sup>257</sup> *Wall*, *Cybercrime: The Transformation of Crime in the Information Age*, supra n. 255.

<sup>258</sup> Regarding the offence see: *Grabosky*, *The Internet, Technology, and Organized Crime*, *Asian Journal of Criminology*, 2007, vol. 2, page 148; *Robertson*, *Identity Theft Investigations*, Kaplan Publishing, 2008, page 43.

<sup>259</sup> Indictment handed down in major ATM skimming operation, Department of Justice, Northern District of Georgia, Press release, 17.02.2009.

nal purposes. Estimated losses to the economy could be up to several billion US dollars a year.<sup>260</sup> There are several links to organized crime groups.<sup>261</sup>

### *Object of the request*

In order for the competent judge from country B to have a complete view about the offender and to deliver the judgment, he or she needs to know the criminal record of the offender. The judge therefore has to transmit a request to country A to see if the offender has or not such a criminal record, and if affirmative, to ask for a transmittal of the copies of those convictions. This piece of information has not been previously solicited by the competent prosecutor from country B.

### *Strategy*

#### Identification of the applicable instruments

The first task is to identify the convention applicable. In this case, due to the fact that both countries are EU members, the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States<sup>262</sup> is applicable, notably Article 6(8)(b), second thesis. Article 6(8) provides that:

The following requests of communication shall be made through the central authority of the MA:

[...]

(b) notices of information from judicial records as referred to in Article 22 of the European Mutual Assistance Convention and Article 43 of Benelux. However, request for copies of convictions and measures as referred to in Article 4 of the Additional Protocol to the European Mutual Assistance Convention<sup>263</sup> may be made directly to the competent authorities.<sup>264</sup>

<sup>260</sup>Final Report of the Model Criminal Code Officers' Committee of the Standing Committee of Attorneys-General, 2006, chapter 3, page 1, available at: [www.scag.gov.au/.../SCAG/...scag...Final\\_Report.../MCLOC\\_MCC\\_Chapter\\_3\\_Identity\\_Crime\\_-\\_Final\\_Report\\_-\\_PDF.pdf](http://www.scag.gov.au/.../SCAG/...scag...Final_Report.../MCLOC_MCC_Chapter_3_Identity_Crime_-_Final_Report_-_PDF.pdf).

<sup>261</sup>*Montaque*, Fraud Prevention Techniques for Credit Card Fraud, Victoria, 2006, page 62; *Choo/Smith*, Criminal Exploitation of Online Systems by Organized Crime Groups, *Asian Journal of Criminology*, 2008, vol. 3, page 41; *Choo*, Organized crimes groups in Cyberspace: A typology, Trends in Organized Crime, *Asian Journal of Criminology*, 2008, vol. 11, page 277; Final Report of the Model Criminal Code Officers' Committee, supra n. 260.

<sup>262</sup>For more details, see the Explanatory Report to the Convention at: [http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229\(02\)&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229(02)&model=guichett). The text of the Convention can be retrieved at: [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0712\(01\):EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0712(01):EN:HTML).

<sup>263</sup>The Second Additional Protocol to the Council of Europe Convention on Mutual Legal Assistance in Criminal Matters from 2001, together with the Explanatory Report and the list of ratifications and declarations can be found online at: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=07/03/2010&CL=ENG>.

<sup>264</sup>Article 4 of the Additional Protocol to the CoE Convention which is brought into discussion refers mainly to the request of criminal records made in individual cases. This situation is applicable to the present case. Article 4 of the Second Additional Protocol has changed Article 22 of European Convention on Mutual Assistance in Criminal Matters 1959, which can be found online at: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CM=8&DF=07/03/2010&CL=ENG>. Recently the Council Framework Decision 2009/315/JHA of 26 February 2009 on the organization and content exchange of information extracted from the criminal record between Member States has been adopted which states in its preamble, paragraph 10 that it will be without prejudice to the possibility of judicial authorities' directly requesting and transmitting information from criminal records in accordance with the previous applicable instruments.

## Channels of communication

The second aspect that needs to be taken into account is what channel of communication is to be followed. In case of urgency, a direct contact between the issuing authority from country B and the executing authority from country A is the best solution available. In this sense, the European Judicial Atlas in Criminal Matter can be used. It is available online.<sup>265</sup> The steps mentioned there should be followed. It should be underlined that this direct contact is not mandatory however, and that the rule is for the transmission to take place through the Ministries of Justice. If a direct contact is not possible, alternative channels still exist, allowing the responsible judge to know exactly how to act in order to get the required information.

If the competent judge from country B does not manage to identify the executing judicial authority from country A and wishes to use the classical rule, the request can be transmitted to the Ministry of Justice of country B which will transmit it to the Ministry of Justice in country A.

Here the choice between the direct channel or through the Ministries of Justice or other relevant central authorities depends also on the domestic legislation of states A and B and how exactly the relevant provisions of Convention of 29 May 2000 on mutual assistance in criminal matters between the Member States were implemented—in this sense, another application developed at EU level can be used, namely the Fiche Belge, which contains reference to the legislation of the Member States on criminal records.<sup>266</sup>

As a last resort in case the competent judge does not manage to identify the executing judicial authority, but still wants to make use of the direct contact and is experiencing difficulties in using the electronic tools, he or she can transmit the request to one of the EJN<sup>267</sup> (European Judicial Network) points of contact. The competent judge can even ask through EJN information about the legal system of the executing state, including whether the executing state accepts the direct contact between the judicial authorities.

## Means of communication

With regard to the means of communication, the use of expedited mean of communication, such as fax or e-mail is recommended, if the request is urgent. If not, a clear assessment has to be done in this respect, and in case the request is regarded of a standard urgency, postal submission could also be acceptable. In the case of a request formulated during trial, it is likely that the issuing judicial authority would need to make use of the expedited means of communication.

### Practical advice

When formulating the request, the summary of the case and the justification of the request need to be clearly specified, as well as the legal provisions relevant in country B.

<sup>265</sup> Refer to: [http://www.ejn-crimjust.europa.eu/atlas\\_advanced.aspx](http://www.ejn-crimjust.europa.eu/atlas_advanced.aspx).

<sup>266</sup> Refer to: [http://www.ejcrimjust.europa.eu/fiches\\_belges\\_result.aspx?measure=405&lang=AT&other](http://www.ejcrimjust.europa.eu/fiches_belges_result.aspx?measure=405&lang=AT&other).

<sup>267</sup> Information about the European Judicial Network can be found at: <http://www.ejn-crimjust.europa.eu/>.

## 2. Second case—“phishing”

*Focus of the case:* Letter rogatory formulated during pre-trial phase, transnational organized crime.

### *Facts of the case*

An organized criminal group from country A sent phishing e-mails to the customers of the auction platform eBay, obtaining as such credit card data of nationals of various countries. The data thus obtained was subsequently used for buying or renting domain names and launching false shipping websites. The eBay clients were encouraged to use the false shipping websites which offered more authenticity to the transactions operated through eBay. In reality the goods were never delivered to the citizens from countries A, B, C, D who paid for the products.

Countries A and B are situated on different continents. There is no bilateral treaty in force between the two countries. Both countries are parties to the UNTOC.

### *Object of the request*

The prosecutor from country A needs to send similar requests to various countries whose citizens have been victimized, including country B. The request to country B refers to the identification of the potential victims. The prosecutor is also soliciting to country B to ask the potential victims if they wish to fill a complaint and if affirmative to transmit the complaint, as well as the details of the offenders held by the potential victims.

### *Strategy*

#### Identifying the applicable convention

The first step in building up the mutual legal assistance request is to identify the applicable legal instrument. In this case, due to the fact that there is neither a bilateral treaty in place between the two states nor other multilateral instrument, the UNTOC becomes relevant.

#### Article 18(7) of the UNTOC

Paragraphs 9 to 29 of this Article shall apply to requests made pursuant to this Article if the States Parties in question are not bound by a treaty of mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 9 to 29 of this Article in lieu thereof. States Parties are strongly encouraged to apply these paragraphs if they facilitate cooperation.

In this sense, the most relevant question that needs to be answered before formulating the request is to verify if the conditions stipulated in Article 18(1) are met in country A. More

specifically, it is especially necessary to verify if computer related fraud and forgery are serious crimes under the domestic legislation of country A.<sup>268</sup>

### Channels of communication

In order to determine which channel of communication is applicable, it is recommended to check the available directories (online directory or the printed version of the directory) and see if a direct contact through the ministries of justice (or other central authorities, e.g., prosecutors' office) is possible. If country B is not allowing a direct contact with its central authority, the prosecutor from country A needs to transmit the request through diplomatic channels.

### Means of communication

The UNTOC in general allows all means of communication, including expedited means thereof. Therefore the transmission via fax should be used if the request is urgent and the requested country allows for such a transmittal. If not, the classical means of communication, mainly post will become applicable.

### The content of the request

When formulating the request, it is highly recommended to make use of the MLA Request Writing Tool<sup>269</sup> and if that is not possible or the issuing judicial authority decides otherwise Article 18(15) of the UNTOC should be taken into consideration.

#### Article 18(15) of the UNTOC

A request for mutual legal assistance shall contain:

- (a) The identity of the authority making the request;
- (b) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;
- (c) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;
- (d) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;
- (e) Where possible, the identity, location and nationality of any person concerned; and
- (f) The purpose for which the evidence, information or action is sought.

<sup>268</sup> For the interpretation of Article 18(1), see Legislative Guides: United Nations Convention Against Transnational Organized Crime, supra n. 139, page 230 et seq. Also see the decisions taken during the meetings of the Working Group on International Cooperation, available at: <http://www.unodc.org/unodc/en/treaties/working-group-on-international-cooperation.html>.

<sup>269</sup> Information about the tool, as well as the tool itself available for download, can be found at: <http://www.unodc.org/mla/>.

### Practical advice

In order to underline the transnational character and achieve a prompter response from the executing state, it is important to stress the fact that there are potential victims in more than one countries, to nominate those countries, to reveal the approximate number of victims and to mention the estimated total amount of prejudice caused (this last piece of information might be relevant for country B especially if it represents the common law system guided by the proportionality principle).

Another important aspect is the language in which the request has to be transmitted. The issuing judicial authority needs to check the declaration country B has made and in this sense the use of online directory of competent national authorities or the printed version of this directory would be of much help.

## 3. Third case—auction fraud

*Focus of the case:* Letter rogatory formulated during the pre-trial phase, non-organized crime, no mutual assistance agreement in place.

### *Facts of the case*

Two offenders, acting from country A, set up a website that looks like the website of a well-known online auction platform. Furthermore, the offenders sent out e-mails containing an attachment with malicious code, which installed spyware when the victim in country B opened the attachment. The offenders used account information obtained from country B's computer to start several auctions offering products that do not exist. The bona fide customers in country C purchased the non-existing goods and transferred the money by using means of electronic payments. The criminal activities were undertaken from IP addresses originating from country A.

Countries A, B and C are in different continents. There is no bilateral treaty in force between the countries. All countries are parties to the UNTOC, but not to the Cybercrime Convention.

### *Background information*

Online auctions are now one of the most popular e-commerce services. In 2006, goods worth more than US\$20 billion were sold on eBay, the world's largest online auction marketplace.<sup>270</sup> Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices. Offenders can exploit the absence of face-to-face contact between sellers and buyers.<sup>271</sup> The difficulty

<sup>270</sup> See: <http://www.ebay.com>.

<sup>271</sup> See Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, *UCLA Journal of Law and Technology*, vol. 6, issue 1.

of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes.<sup>272</sup> The two most common scams include:<sup>273</sup>

- Offering non-existent goods for sale and requesting buyers to pay prior to delivery;<sup>274</sup>
- Buying goods and asking for delivery, without intention to pay.

In response, auction providers have developed protection systems such as the feedback/comments system. After each transaction, buyer and sellers leave feedback for use by other users<sup>275</sup> as neutral information about the reliability of sellers/buyers. However, criminals have responded and circumvented this protection by using accounts from third parties.<sup>276</sup> In this scam called “account takeover”,<sup>277</sup> offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

### *Object of the request*

Internet providers, such as e-mail providers, online shops and auction platforms, often keep records of access to their services in so-called log-files. To be able to identify the offenders acting from country A, the prosecutor in country C needs to request the submission of log-files from country B in order to identify the Internet user who used the IP addresses to access the auction platform account. To ensure that the evidence is not deleted prior to the execution of the requested act, provisional measures need to be considered.

#### **Practical advice**

Identity-related crime nowadays involves digital evidence to a large degree. Collecting such evidence presents unique challenges. One of the most important challenges is the fact that data that could become relevant for an investigation might be automatically deleted within days if not relevant for billing purposes. Therefore immediate response and the request for provisional measure have a high priority.

### *Strategy and identification of other applicable instruments*

The first step is the identification of applicable instruments for mutual assistance. Although country B and country C are parties to the UNTOC and this Convention offers a wide range of means of international cooperation the Convention is in the current case not applicable. Based on Article 3(1), the provisions of the Convention are only applicable if

<sup>272</sup>The United States Internet Crime Complaint Centre (IC3) (a partnership between the FBI and the National White Collar Crime Centre) reported that around 45 per cent of complaints refer to auction fraud. See: “IC3 Internet Crime Report 2006”, available at: [http://www.ic3.gov/media/annualreport/2006\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf).

<sup>273</sup>“Law Enforcement Efforts to combat Internet Auction Fraud”, Federal Trade Commission, 2000, page 1, available at: <http://www.ftc.gov/bcp/reports/int-auction.pdf>.

<sup>274</sup>See *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on Aging, 2004, page 7, available at: <http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf>.

<sup>275</sup>For more information, see, for example: <http://pages.ebay.com/help/feedback/feedback.html>.

<sup>276</sup>Regarding the criminalization of “account takeovers”, see *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

<sup>277</sup>See “Putting an End to Account-Hijacking Identity Theft”, Federal Deposit Insurance Corporation, 2004, available at: [http://www.fdic.gov/consumers/consumer/idtheftstudy/identity\\_theft.pdf](http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf).

the offence involves an organized crime group. Article 2 defines an organized criminal group as a structured group of three or more people, which, in the above-mentioned scenario, is not the case.

### Article 2 of the UNTOC

#### *Use of terms*

For the purposes of this Convention:

- (a) "Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

### Article 3 of the UNTOC

#### *Scope of application*

1. This Convention shall apply, except as otherwise stated herein, to the prevention, investigation and prosecution of:
  - (a) The offences established in accordance with Articles 5, 6, 8 and 23 of this Convention; and
  - (b) Serious crime as defined in Article 2 of this Convention; where the offence is transnational in nature and involves an organized criminal group.

Given the absence of applicable international conventions and the lack of mutual assistance agreements, the request needs to be transmitted using the rules of international courtesy, and on the basis of the principle of reciprocity.<sup>278</sup>

### Channels and means of communication

Based on the rules of international courtesy, the requesting state needs to transmit a request through the diplomatic channels to the executing state. In practice, this generally means that a judicial authority of country C will have to send the letter rogatory to its Ministry of Justice which will forward the request to the Ministry of External Affairs in country C. The It will then transmit the request to the Ministry of Foreign Affairs in country B which will forward the request to the Ministry of Justice of country B. Finally, the latter will communicate the letter rogatory to the authority competent to execute the request.

<sup>278</sup> See, in this regard, *Pop*, *The Principle and General Rules of the International Judicial Cooperation in Criminal Matters*, *AGORA International Journal of Juridical Science*, 2008, page 160 et seq.; *Stowell*, *International Law: A Restatement of Principles in Conformity with Actual Practice*, 1931, page 262; *Recueil Des Cours*, *Collected Courses*, Hague Academy of International Law, 1976, page 119.



### Practical advice

Compared to a direct contact or contacts through central contact authorities, the submission of requests through diplomatic channels are time consuming and could cause serious impediments to the investigation—especially with regard to urgent cases. Requests for provisional measures will therefore likely not be as effective as through other channels.

The requesting authority should therefore check—as with regard to the fact that country B is party to the UNTOC—if previous requests have been submitted to country B, in order to find out if country B normally accepts the use of expedited means of communication. If this is the case, an informal request could be sent to the contact points responsible for requests based on the UNTOC to find out if requests transmitted using the rules of international courtesy, based on reciprocity can be submitted in advance via e-mail or fax with the certified original documents following through diplomatic channels. Some countries accept this procedure.

### Content of the request

The request submitted to country B needs to contain certain key information. As both (the requesting and the executing state) are parties to the UNTOC, the related regulation in the Convention (Article 18) can, despite the fact that the Convention is not applicable, be used as a guideline.

#### Article 18(15) of the UNTOC

15. A request for mutual legal assistance shall contain:
- (a) The identity of the authority making the request;
  - (b) The subject matter and nature of the investigation, prosecution or judicial proceeding to which the request relates and the name and functions of the authority conducting the investigation, prosecution or judicial proceeding;
  - (c) A summary of the relevant facts, except in relation to requests for the purpose of service of judicial documents;
  - (d) A description of the assistance sought and details of any particular procedure that the requesting State Party wishes to be followed;
  - (e) Where possible, the identity, location and nationality of any person concerned; and
  - (f) The purpose for which the evidence, information or action is sought.

Following the procedures of the UNTOC will ensure that the request is in line with the procedures that were already implemented to domestic legislation of country A and practiced by the competent authorities.

### Practical advice

If there is uncertainty with regard to the procedures it can be useful to contact the executing state prior to sending the formal request or to undertake research to find out if there are specific requirements that need to be taken into account. In this context, the online directory of competent national authorities is very helpful.

## Follow-up

After the submission of information by country B, the authorities in country C need to undertake further approaches to identify the offenders. Based on the IP address and log-file information submitted by country B, another requests needs to be submitted—this time to country A.

## 4. Fourth case—account takeover

*Focus of the case:* Letter rogatory formulated during the pre-trial phase, non-organized crime.

### *Facts of the case*

The victim is based in country A and has an e-mail account with a company located in country B. An offender has taken over the e-mail account by illegally accessing the victim's mail server in order to send out e-mails appearing to be sent by the victim. Country A and country B are situated on different continents. The countries are not parties to the Council of Europe Cybercrime Convention.<sup>279</sup> Instead, a bilateral treaty is applicable.

### *Background information*

Account takeover is a phrase used to describe the illegal use of the victims account.<sup>280</sup> It is one of the traditional identity-related offences.<sup>281</sup> The offenders target accounts such as checking accounts and e-mail accounts, but also user accounts for action platforms and social networks.<sup>282</sup> By taking over the account, the offenders are able to use the identity of the victim—for example, by sending out e-mails from the victim's e-mail account or transferring money from the victim's bank account. The offenders acting in this manner make extensive use of the fact that access to the account gives legitimacy to the transaction. Offenders can use account takeover to circumvent protection measures implemented by providers to hinder the fraudulent use of services. One example is the implementation of feedback/comments systems on auction platforms. To avoid users abusing the service, some auction platforms enable customers to evaluate their counterpart. After each transaction, buyer and sellers leave feedback for use of other users<sup>283</sup> as neutral information about the reliability of sellers/buyers. This makes it more difficult for criminals to use

<sup>279</sup>For more details about the Convention, see *Sofaer*, Toward an International Convention on Cybercrime, in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, available at: [http://media.hoover.org/documents/0817999825\\_221.pdf](http://media.hoover.org/documents/0817999825_221.pdf); *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, *Computer Law Review International*, 2006, page 140 et seq.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, *ibid*, page 7 et seq.; *Jones*, The Council of Europe Convention on Cybercrime; *Broadhurst*, Development in the global law enforcement of cyber-crime, page 408 et seq.

<sup>280</sup>*Biegelman*, Identity Theft Handbook, Detection, Prevention and Security, John Wiley & Sons, Inc., 2009, page 29.

<sup>281</sup>*Hoofnagle*, Identity Theft: Making the Known Unknowns Known, *Harvard Journal of Law & Technology*, 2007, page 103.

<sup>282</sup>*Ferretti*, The Law and Consumer Credit Information in the European Community, The Regulation of Credit Information Systems, page 26; *Hoofnagle*, Identity Theft, *supra*.

<sup>283</sup>For more information, see, for example: <http://pages.ebay.com/help/feedback/feedback.html>.

auction platforms to commit crimes. However, criminals have circumvented this protection by using accounts of third parties.<sup>284</sup> In this approach of “account takeover”,<sup>285</sup> offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

### *Object of the request*

After the account takeover was reported by the victim, the local authorities in country A need to get access to evidence that enables them to trace back the offender. In this context, log-in information from the e-mail provider is particularly relevant. Providers often keep records of IP addresses used by customers accessing their account. Receiving the IP address might enable the local authorities in country A to identify the offender. With regard to the fact that the fundamental principle of national sovereignty does not permit investigations within the territory of another country without the permission of local authorities,<sup>286</sup> the investigator based in country A cannot simply collect evidence remotely. The fact that many Internet services such as e-mail accounts or membership in social networks are offered globally highlights the importance of close cooperation between the countries involved in the investigation.<sup>287</sup>

### *Strategy*

The first step is the identification of applicable instruments. Given that there is no indication that more than one offender was involved, the UNTOC is not applicable as the definition of organized crime in Article 2(a) requires a group of three or more persons. As the crime is committed by using information technology and required the illegal access to a computer system, the application of instruments contained in the Council of Europe Cybercrime Convention<sup>288</sup> could in general be taken into consideration. The regulations in the Convention are only applicable for countries that ratified the instrument. As in the current case country A and country B are not parties to it, the means of international cooperation mentioned there are not applicable either.

### *Bilateral treaty*<sup>289</sup>

In investigations like this, the focus will be on the preservation of evidence. Unlike the Convention on Cybercrime, which allows for mutual assistance regarding provisional

<sup>284</sup> Regarding the criminalization of “account takeovers”, see *Gercke*, supra n. 276, page XIV.

<sup>285</sup> See “Putting an End to Account-Hijacking Identity Theft”, supra n. 277.

<sup>286</sup> Regarding the principle of National Sovereignty, see *Roth*, State Sovereignty, International Legality, and Moral Disagreement, supra n. 25; *Martinez*, National Sovereignty and International Organizations, 1996; *Riegler*, Nation Building Between National Sovereignty and International Intervention, 2005.

<sup>287</sup> Regarding the need for international cooperation in the fight against Cybercrime, see *Putnam/Elliott*, International Responses to Cyber Crime, supra n. 25, page 35 et seq.

<sup>288</sup> For more details about the Convention, see *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, page 140 et seq.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.; *Jones*, The Council of Europe Convention on Cybercrime; *Broadhurst*, Development in the global law enforcement..., page 408 et seq.

<sup>289</sup> The following section will be based on the Model Treaty on Mutual Assistance in Criminal Matters, adopted by General Assembly resolution 45/117, subsequently amended by General Assembly Resolution 53/112.

measures,<sup>290</sup> mutual assistance agreements, such as those considering the Model Treaty on Mutual Assistance in Criminal Matters, do not contain such provisional measures.<sup>291</sup> A number of recent agreements contain provisional measures in addition to traditional measures.

The request needs to be sent to the designated contact point. Following the provisions established in Article 3 Model Treaty on Mutual Assistance in Criminal Matters, the requests need to be submitted to the central authority, unless countries consider providing direct communication. The request needs to contain information as specified in the agreement (see, for example, Article 5 Model Treaty on Mutual Assistance in Criminal Matters).

### Article 5 of the Model Treaty on Mutual Assistance in Criminal Matters

#### *Content of requests*

1. Requests for assistance shall include:
  - (a) The name of the requesting office and the competent authority conducting the investigation or court proceedings to which the request relates;
  - (b) The purpose of the request and a brief description of the assistance sought;
  - (c) A description of the facts alleged to constitute the offence and a statement or text of the relevant laws, except in cases of a request for service of documents;
  - (d) The name and address of the person to be served, where necessary;
  - (e) The reasons for and details of any particular procedure or requirement that the requesting State wishes to be followed, including a statement as to whether sworn or affirmed evidence or statements are required;
  - (f) Specification of any time-limit within which compliance with the request is desired;
  - (g) Such other information as is necessary for the proper execution of the request.

The means of communication depend on the regulation in the agreement. If expedited means of communication are not explicitly mentioned, traditional methods of submission are in general necessary. Special attention should also be paid to requirements related to the language of the request.<sup>292</sup>

## 5. Fifth case—skimming

*Focus of the case:* Transnational organized criminal group, letter rogatory during the pre-trial stage, UNTOC, European Union and Council of Europe instruments.

<sup>290</sup> See Article 29 of the Convention on Cybercrime, supra n. 117.

<sup>291</sup> See Article 1 Model Treaty on Mutual Assistance in Criminal Matters.

<sup>292</sup> See, for example, Article 5(3) Model Treaty on Mutual Assistance in Criminal Matters.

### *Facts of the case*

An organized criminal group based in country A installed skimming devices on ATMs situated in country B and country C. By using manipulated key pads and card slots and a micro-camera, they obtained credit card information and personal identification number (PIN). Later, based on that data, they have created cloned credit cards and used them in order to make fraudulent transactions.

Country A, country B and country C are European countries. All countries are parties to the UNTOC, and countries A and B are members of the European Union. Country A and country C are members of the Council of Europe.

### *Background information*

The term “skimming” is in general used to describe an offence where the offenders manipulate an ATM in order to obtain credit card information and personal identification numbers.<sup>293</sup> It is a two phase offence. In the first phase offenders obtain credit card information by adding hardware to an ATM. In general devices are covertly fitted over the ATM’s card slot. They are designed to look like a part of the machine.<sup>294</sup> The device records and stores the details of all cards as they are inserted. To get into possession of the personal identification number (PIN) offenders either use manipulated keypads or pinhole camera to record the customer using the ATM and entering their PIN.<sup>295</sup> In the second phase, the offenders use the obtained information to clone credit cards and use them. Estimated losses to the economy could be up to several billion US dollars a year.<sup>296</sup> There are several links to organized criminal groups.<sup>297</sup>

#### **Practical advice**

The involvement of an organized criminal group is especially relevant for the application of the UNTOC.

### *Object of the request*

The prosecutor in country A seeks the following information: the names of the banks which issued the credit cards that were cloned, the owners of the credit cards and the total amount of the damage caused to the victims. He sends out requests with similar objects to countries B and country C in order to receive the information.

<sup>293</sup> Regarding the offence, see *Grabosky*, *The Internet, Technology, and Organized Crime*, supra n. 261, page 43.

<sup>294</sup> Indictment handed down in major ATM skimming operation, Department of Justice, Northern District of Georgia, press release, 17.02.2009.

<sup>295</sup> ATM Crime, ENISA (European Network and Information Security Agency), 2009, page 14, available at: <http://www.scribd.com/doc/19636432/Enisa-Atm-Crime>.

<sup>296</sup> Final Report of the Model Criminal Code Officers’ Committee of the Standing Committee of Attorneys-General, supra n. 260.

<sup>297</sup> *Montaque*, *Fraud Prevention Techniques for Credit Card Fraud*, supra n. 261, page 62; *Choo/Smith*, *Criminal Exploitation of Online Systems by Organized Crime Groups*, page 41; *Choo*, *Organized crimes groups in Cyberspace...*, supra n. 261, page 277; Final Report of the Model Criminal Code Officers’ Committee of the Standing Committee of Attorneys-General, supra n. 260.

## Strategy

The first step is the identification of applicable international instruments. As this case features elements of organized crime, the UNTOC needs to be taken into consideration. However, in relation to Article 18, paragraphs 6 and 7, it is necessary to investigate first if other treaties that govern mutual legal assistance are applicable. For this investigation such treaties are particularly relevant given that all three countries are located in the same region.

### Article 18 of the UNTOC

#### *Mutual legal assistance*

[...]

6. The provisions of this article shall not affect the obligations under any other treaty, bilateral or multi-lateral, that governs or will govern, in whole or in part, mutual legal assistance.

7. Paragraphs 9 to 29 of this article shall apply to requests made pursuant to this article if the States Parties in question are not bound by a treaty of mutual legal assistance. If those States Parties are bound by such a treaty, the corresponding provisions of that treaty shall apply unless the States Parties agree to apply paragraphs 9 to 29 of this article in lieu thereof. States Parties are strongly encouraged to apply these paragraphs if they facilitate cooperation.

## Identification of other applicable instruments

As States A and B are members of the European Union, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000)<sup>298</sup> is applicable, unless one of the countries involved has not yet ratified the Convention.<sup>299</sup> After four years of intensive negotiation,<sup>300</sup> the Convention was finalized in 2000 and entered into force in 2005, replacing the Framework Decision on Joint investigation teams<sup>301</sup> and supplements the Council of Europe instruments.<sup>302</sup>

With regard to country C, it should be kept in mind that both country A and country C are members of the Council of Europe. As a consequence, the Council of Europe Convention on Mutual Assistance in Criminal Matters (1959) is applicable.<sup>303</sup> The Convention was ratified by all 47 member states of the Council of Europe and Israel as a non-member.<sup>304</sup> As with relates to the means of communication, it is also important to check if country A and country C are also parties to the Second Additional Protocol of 2001 to the

<sup>298</sup> Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Official Journal* 197, 12/07/2000, pages 3-23.

<sup>299</sup> For a general overview about the Convention, see *Bantekas/Nash*, *International Criminal Law*, supra n. 57, page 237 et seq.

<sup>300</sup> *Maklu-Uitgevers in De Ruyver/Bermeulen/Vander Beken*, *Combating Transnational Organized Crime*, 2002, page 224.

<sup>301</sup> Framework Decision 2002/465/JHA.

<sup>302</sup> *Kronenberger/Kapteyn* (eds), *The European Union and the International Legal Order—Discord or Harmony*, European Free Trade Association, 2001, page 547.

<sup>303</sup> European Convention on Mutual Assistance in Criminal Matters (ETS 30).

<sup>304</sup> The status of ratification of Council of Europe Conventions is available at: <http://conventions.coe.int>.

Mutual Legal Assistance Convention.<sup>305</sup> The Protocol, ratified as of December 2009 by 19 countries, contains special regulations related to the channels of communication.<sup>306</sup>

### Practical advice

The status of ratification of Council of Europe instruments, the text of the instruments and explanatory reports are available online at: <http://conventions.coe.int>.

## Channels of communication

For the purposes of initial contact, the selection of the channels of communication is of great importance. Depending on which instrument is applicable, the channels of communication used by country A to communicate with country B and country C can be different.

Concerning the communication between countries A and B, there can in general be a direct contact between the prosecutor's offices in the two countries, in accordance with the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.<sup>307</sup>

### Article 6 of the 2000 EU MLA Convention

#### *Transmission of requests for mutual assistance*

1. Requests for mutual assistance and spontaneous exchanges of information referred to in Article 7 shall be made in writing, or by any means capable of producing a written record under conditions allowing the receiving Member State to establish authenticity. Such requests shall be made directly between judicial authorities with territorial competence for initiating and executing them, and shall be returned through the same channels unless otherwise specified in this Article. Any information laid by a Member State with a view to proceedings before the courts of another Member State within the meaning of Article 21 of the European Mutual Assistance Convention and Article 42 of the Benelux Treaty may be the subject of direct communications between the competent judicial authorities.

2. Paragraph 1 shall not prejudice the possibility of requests being sent or returned in specific cases:

- (a) between a central authority of a Member State and a central authority of another Member State; or
- (b) between a judicial authority of one Member State and a central authority of another Member State.

[...]

4. Any request for mutual assistance may, in case of urgency, be made via the International Criminal Police Organisation (Interpol) or any body competent under provisions adopted pursuant to the Treaty on European Union.

[...]

<sup>305</sup> Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS 182).

<sup>306</sup> See especially Article 4.

<sup>307</sup> See Article 6 for details.

Contact through other authorities can be necessary if one of the countries has declared that it will continue to apply the communication through the central authority. In urgent cases the Convention also allows transmissions to be submitted through Interpol.<sup>308</sup> As the Convention only supplements other instruments, such as those from the Council of Europe,<sup>309</sup> other legal instruments could become relevant for those member states of the EU that did not ratify the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

### Practical advice

There is an online application that can be used to identify the competent authority in European countries.<sup>310</sup>

The above Convention cannot be used to select the channels of communication between country A and country C, as both are not Member States of the European Union. However, as both countries are members of the Council of Europe, the channels of communication will be identified on the basis of the Council of Europe Convention on Mutual Assistance in Criminal Matters (1959). In accordance with Article 15 of the Convention, the request should be submitted to the designated central authority, in this case the Ministry of Justice. Only in urgent cases will a direct contact with the judicial authority in country C be possible. However even in such cases, the response must still come through the central authority.

### Article 15 of the 1959 MLA Convention

Letters rogatory referred to in Articles 3, 4 and 5 as well as the applications referred to in Article 11 shall be addressed by the Ministry of Justice of the requesting Party to the Ministry of Justice of the requested Party and shall be returned through the same channels. In case of urgency, letters rogatory may be addressed directly by the judicial authorities of the requesting Party to the judicial authorities of the requested Party. They shall be returned together with the relevant documents through the channels stipulated in paragraph 1 of this Article.

Direct contact between judicial authorities outside urgent cases is only possible if both countries are parties to the Second Additional Protocol to the Council of Europe Convention. In this case, the documents on the accomplishment of the request will also be returned through the direct contact.<sup>311</sup> This provision will apply, unless one of the countries has made declarations that it will continue to apply the transmission through the central authorities.

<sup>308</sup> Ibid.

<sup>309</sup> *Kronenberger/Kapteyn* (eds), *The European Union and the International Legal Order—Discord or Harmony*, European Free Trade Association, 2001.

<sup>310</sup> See: [http://www.ejn-crimjust.europa.eu/atlas\\_advanced.aspx](http://www.ejn-crimjust.europa.eu/atlas_advanced.aspx).

<sup>311</sup> Article 4(1) of the Second Additional Protocol to the CoE 1959 Convention.



### Practical advice

The example shows that the selection of the channels of communication even within one region (Europe) is challenging as different legal frameworks apply. The online application is a useful tool to identify the right competent authorities. Investigations of skimming cases showed that crime groups often not only act in one country, but different countries. As a consequence, the procedures related to international cooperation and especially the selection of channels for the transmission of the request are of great practical relevance. If direct contact is possible, it should be used, as this in general speeds up the process.

### Means of communication

Formal aspects of the proceedings are equally challenging as the selection of the channels of communication. Based on the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, the means of communication available between country A and country B range from delivery via post to fax and e-mail, as in addition to traditional means of communication, the Convention also covers expedited means of communication.<sup>312</sup>

Based on the Council of Europe Convention on Mutual Assistance in Criminal Matters, communication between countries A and C is limited to the regular means of communication, which is delivery by post, as the text of the Convention does not explicitly mention expedited means of communication. The Second Addition Protocol, however, explicitly mentions such means of communication.

#### Second Additional Protocol to COE MLA Convention

##### Article 4. Channels of communication

[...]

9. Requests for mutual assistance and any other communications under this Convention or its Protocols may be forwarded through any electronic or other means of telecommunication provided that the requesting Party is prepared, upon request, to produce at any time a written record of it and the original. However, any Contracting State, may by a declaration addressed at any time to the Secretary-General of the Council of Europe, establish the conditions under which it shall be willing to accept and execute requests received by electronic or other means of telecommunication.

[...]

Nonetheless, as mentioned in Article 4, the contracting States may establish certain conditions in relation to the use of electronic or other means of telecommunication.

<sup>312</sup>For more details see the Explanatory Report to the Convention, available at: [http://eur-lex.europa.eu/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229\(02\)&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=42000Y1229(02)&model=guichett).

### Practical advice

As a consequence of the ability of Member States to restrict means of expedited communication, it is necessary to check possible reservations of requested states prior to making use of means of electronic communication. The declarations submitted are available at: <http://conventions.coe.int>.

### Content of the request

The request submitted to countries A and B needs to contain certain key information. Very often the competent authorities dealing with such requests have a set of standard forms that fulfil the requirements of the requested state. As each state's requirements are different, it is difficult to provide a standard form for all possible recipients, but there are a number of issues that should in general be taken into consideration:

- The request generally needs to contain essential information, such as the name of the authority that is making the request, the object of the request and reason, identity and the nationality of the person concerned;
- To ensure that the requested state is able to respond in a timely manner, the transnational character of the offence should be highlighted;
- It is necessary that all relevant details are described. This is especially relevant for cases of identity-related crime, as those cases are often very complex. An overview should be submitted of all facts that are relevant for the requested state to understand the background of the request;
- It is important that applicable domestic legal provisions are mentioned. This is particularly relevant in cases where the requested party applies the principle of dual criminality.<sup>313</sup> Dual criminality might be one of the conditions for executing the request. In this case, it could be more than useful to submit a copy of the local legislation to facilitate the process of evaluating dual criminality.

## 6. Sixth case—skimming II

*Focus of the case:* Letter rogatory formulated during pre-trial phase. MLA preceding the extradition request. Transnational organized crime component.

<sup>313</sup>Dual criminality exists if the offence is a crime under both the laws of the requested and requesting parties. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Article 2 of the EU Framework Decision of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see *United Nations Manual on the Prevention and Control of Computer-Related Crime*, 269, available at: <http://www.uncjin.org/Documents/EighthCongress.html>; *Schjolberg/Hubbard, Harmonizing National Legal Approaches on Cybercrime*, 2005, page 5, available at: [http://www.itu.int/osg/spu/cybersecurity/presentations/session12\\_schjolberg.pdf](http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf).

### *Facts of the case*

An offender from country B is involved in an organized criminal group which allegedly committed computer-related fraud and forgery, followed by credit card cloning offences, in countries A, C, D and E. The above has caused damage to multiple victims in the above-mentioned countries. The MLA request comes from country A to country B. Both States are parties to the UNTOC. There is no other multilateral or bilateral treaty applicable between the two countries.

### *Background information*

The term “skimming” is in general used to describe an offence where the offenders manipulate an ATM in order to obtain credit card information and personal identification numbers.<sup>314</sup> It is a two-phase offence. In the first phase, offenders obtain credit card information by adding hardware to an ATM. In general devices are covertly fitted over the ATM’s card slot, designed to look like a part of the machine.<sup>315</sup> The device records and stores the details of all cards as they are inserted. To gain possession of the personal identification number (PIN), offenders use either manipulated keypads or a pinhole camera to record the customer using the ATM and entering their PIN.<sup>316</sup> In the second phase, the offenders use the obtained information to close credit cards and use them. Estimated losses to the economy could be up to several billion US dollars a year.<sup>317</sup> There are several links to organized crime groups.<sup>318</sup>

Fraud is an offence typically related to cybercrime nowadays, as information technology offers advanced opportunities for fraud. Credit card fraud,<sup>319</sup> advance fee fraud,<sup>320</sup> Internet marketing and retail fraud and auction fraud<sup>321</sup> are just some examples of methods used in relation to Internet technology.

<sup>314</sup> Regarding the offence, see *Grabosky*, The Internet, Technology, and Organized Crime, supra n. 261, page 43.

<sup>315</sup> Indictment handed down in major ATM skimming operation, Department of Justice, Northern District of Georgia, press release, 17.02.2009.

<sup>316</sup> ATM Crime, ENISA, supra n. 298, page 14.

<sup>317</sup> Final Report of the Model Criminal Code Officers’ Committee of the Standing Committee of Attorneys-General, supra n. 260.

<sup>318</sup> *Montaque*, Fraud Prevention Techniques for Credit Card Fraud, supra n. 261, page 62; *Choo/Smith*, Criminal Exploitation of Online Systems by Organized Crime Groups, *Asian Criminology*, 2008, vol. 3, page 41; *Choo*, Organized crimes groups in Cyberspace..., page 277; Final Report of the Model Criminal Code Officers’ Committee of the Standing Committee of Attorneys-General, supra n. 260.

<sup>319</sup> Regarding the extend of credit card fraud, see Consumer Fraud and Identity Theft Complain Data, January–December 2005, Federal Trade Commission, 2006, page 3, available at: <http://www.consumer.gov/sentinel/pubs/Top-10Fraud2005.pdf>.

<sup>320</sup> The term “advance fee fraud” describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see *Reich*, Advance Fee Fraud Scams in-country and across borders, *Cybercrime & Security*, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, “Trends & Issues in Crime and Criminal Justice”, No. 121, available at: <http://www.aic.gov.au/publications/tandi/ti121.pdf>; *Oriola*, “Advance fee fraud on the Internet: Nigeria’s regulatory response”, *Computer Law & Security Report*, vol. 21, issue 3, page 237; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on Aging, supra n. 273, page 7.

<sup>321</sup> The term “auction fraud” describes fraudulent activities involving electronic auction platforms over the Internet. Regarding auction fraud, see *Bywell/Oppenheim*, Fraud on Internet Auctions, *Aslib Proceedings*, 53 (7), page 265 et seq., available at: <http://www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf>; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, *Federal Communications Law Journal*, 52 (2), page 453 et seq.; *Chau/Faloutsos*, Fraud Detection in Electronic Auction, available at: [http://www.cs.cmu.edu/~dchau/papers/chau\\_fraud\\_detection.pdf](http://www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf); *Dolan*, Internet Auction Fraud: The Silent Victims, *Journal of Economic Crime Management*, vol. 2, issue 1, available at: <https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf>.

### Practical advice

The involvement of an organized criminal group is especially relevant for the application of the UNTOC.

### *Object of the request*

The authorities from country A have information that the offender, situated in country B, will try to flee from country B. They need to make sure that the incriminating evidence they believe might exist in his or her possession is conserved and, if confirmed, in a second phase, to ask for the provisional arrest. It would allow them to submit an extradition request. Therefore, they need to ask to the judicial authorities in country B to execute a house search and a computer search at the offender's domicile. Due to the fear that the offender intends to leave country B and abscond from justice, the MLA request has an urgent character.

### *Strategy*

Both countries are parties to the UNTOC and, as previously mentioned, there is no bilateral or other multilateral treaty applicable. Therefore the request will be formulated on the basis of the UNTOC. The request is of an urgent nature as there are strong indications to believe that the offender will leave country B.

### Article 18(13) of the UNTOC

13. Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the State Parties. This requirement shall be without prejudice to the right of a State Party to require that such requests and communications be addressed to it through diplomatic channels, and, in urgent circumstances, where the State Parties agree, through the International Criminal Police Organization, if possible.

### Transmission of the request

The judicial authorities from country A have to first check if they want to transmit the request through Interpol. If country B permits such transmissions, in this sense the directory of competent national authorities is of utmost importance. It cannot be assumed that the Interpol channel is accepted by all the countries party to the UNTOC. Some of them explicitly mention that, in urgent cases, they do not accept transmittal through Interpol, therefore such a check is a necessary step.

A second aspect that needs to be taken into account is that the decision to choose this channel belongs to the judicial authority. A strong incentive to do so would be if the requested State accepts requests through diplomatic channels, which would not be the most suitable way to proceed in the given circumstances. Transmission through Interpol

would normally facilitate the contact between the judicial authority in country A and the executing one in country B.

### Execution of the request

The national Interpol office of the requested State should consequently transmit the request directly to the competent judicial authority, which needs to execute it and avoid, as much as possible, creating an additional link by submitting the request to the central authority of the requested State (unless there are specific domestic provisions that compels them to do so).

### Follow-up

After the execution of the request, the answer should be transmitted directly by the executing judicial authority to the requesting judicial authority through expedited means of communication or, if direct contact is not possible, again through Interpol. Based on the evidence gathered, country A may subsequently forward an extradition request.

#### Practical advice

Article 18(17) of the UNTOC stipulates that the request has to be executed in accordance with the domestic law of the requested State, to the extent possible and as long as it does not contradict it, in accordance with the procedures mentioned in the request. Therefore, it has to be retained that Interpol is only a channel of communication and the formal requirements for submitting and executing a request remain valid.

## 7. Seventh case—smuggling of migrants

*Focus of the case:* Letter rogatory formulated during pre-trial phase, organized crime component

### *Facts of the case*

Offenders from country A are involved in an organized criminal group involved in the smuggling of migrants—citizens of country C—from country A to country B using synthetic identities,<sup>322</sup> but also, occasionally, real identities obtained by altering legitimate ID cards. Countries A and B are neighbouring countries. Country C is located in another continent. All three countries are parties to UNTOC and the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the UNTOC. Between countries A and B there is also a bilateral treaty in force with regard to international judicial cooperation in criminal matters.

<sup>322</sup>A synthetic identity is obtained by putting together real and fake data or entirely fake data. For more details regarding the synthetic identities, see *McFadden*, Detecting synthetic identity fraud, available at: [http://www.bankrate.com/brm/news/pf/identity\\_theft\\_20070516\\_a1.asp](http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp). See also *Gercke*, Legal Approaches to Criminalize Identity Theft, *supra* n. 28, page 39.

### *Object of the request*

The authorities from country B, which are conducting the investigation, need to know different pieces of information: with regard to country A they need to receive data about the organized criminal group and its modus operandi, with special emphasis on previous criminal activities/previous convictions (if applicable); from country C the authorities need to obtain the real identification data about the smuggled migrants, due to the fact that the documents produced before the authorities of country B do not correspond to their real identities.

### *Strategy*

The formal request comes as a consequence of previous informal cooperation between law enforcement agencies which is allowed by Articles 27 and 28 of the UNTOC, as well as Article 10 of the Smuggling of Migrants Protocol, and which is also normally allowed by modern bilateral treaties. As previously mentioned in chapter II, this kind of cooperation, whether police-police cooperation or law enforcement agencies cooperation in general, is vital in getting the first inputs in the criminal investigations, which are the main elements that allow further construction of a formal MLA request.

#### Article 10 of the Smuggling of Migrants Protocol

##### *Information*

1. Without prejudice to Articles 27 and 28 of the Convention, States Parties, in particular those with common borders or located on routes along which migrants are smuggled, shall, for the purpose of achieving the objectives of this Protocol, exchange among themselves, consistent with their respective domestic legal and administrative systems, relevant information on matters such as:

- (a) Embarkation and destination points, as well as routes, carriers and means of transportation, known to be or suspected of being used by an organized criminal group engaged in conduct set forth in Article 6 of this Protocol;
- (b) The identity and methods of organizations or organized criminal groups known to be or suspected of being engaged in conduct set forth in Article 6 of this Protocol;
- (c) The authenticity and proper form of travel documents issued by a State Party and the theft or related misuse of blank travel or identity documents;
- (d) Means and methods of concealment and transportation of persons, the unlawful alteration, reproduction or acquisition or other misuse of travel or identity documents used in conduct set forth in Article 6 of this Protocol and ways of detecting them;

[...]

### **Channels and means of communication**

In order to make the formal cooperation possible, country B will have to observe with reference to country A the provisions of the bilateral treaty, bearing in mind Article 18(7) which confers, as mentioned in previous occasions, pre-eminence to pre-existent bilateral treaties. For details on bilateral treaties, see the fourth case above.

With reference to the request submitted by country B to country C, the UNTOC and the Smuggling of Migrants Protocol are applicable and should be invoked jointly. The rules provided in Article 18 referring to the channels of communication and further formal requirements, should be observed (see previous cases for details).

As mentioned before, Article 18(9) establishes as an optional ground of refusal to execute MLA requests, the absence of dual criminality. However, in the present case, the request cannot be refused in normal circumstances based on this reason, as both countries B and C are parties to the Smuggling of Migrants Protocol. It means that they have implemented in their domestic legislation Article 6 of the Protocol, which criminalizes not only the smuggling of migrants per se, but also the producing/procuring/providing fraudulent travel or identity documents with the purpose of enabling the smuggling of migrants. The success of the request depends also on the partial or total implementation of the substantive criminal law provisions in the requested State.

### Content of the request

In terms of the content of the request, the conditions provided in Article 18(15) should be observed, but also the specific requirements of the requested State, if they are known (previous experience with that State and data obtained through the informal cooperation should be used). This example highlights from a practical point of view the interrelationship between the substantive, procedural and international cooperation provisions of the UNTOC and its Protocols, as well as the importance of implementing the legislation of each of the cooperating States.

## 8. Eighth case—forgery

*Focus of the case:* MLA request formulated during trial phase. Transnational organized crime component.

### *Facts of the case*

Offenders from country A have committed computer-related crime and forgery in an organized manner, causing prejudices to victims situated in countries B, C, D, E, F, and G. Countries A, B and C are in Europe, D and E in South America, F in North America and G in Australia. Countries A and B are parties to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000) and countries A and C are parties to the Council of Europe Convention 1959. All the countries involved are parties to the UNTOC. Between countries A and F there is an applicable bilateral treaty. Countries A, B and F are parties to the Cybercrime Convention 2001.

### *Object of the request*

The judge from country A needs to send service of documents to countries B, C, D, E, F, G. This request during trial stage is the last one in a chain of cooperation, starting with

complaints submitted by victims to their national authorities or directly to authorities from country A, police cooperation, and formal requests submitted during the pre-trial stage in which rogatory letters have been sent to countries B, C, D, E, F, G in order to establish the identity of the victims and to get their statements and all other additional documents retained as evidence to prepare the indictment against the components of the organized criminal group. In the trial phase, the injured parties need to be informed about the term of the trial and about the fact that they can be present in court, if they wish so.

### *Strategy—considerations on the applicability of relevant instruments*

In this particular case, due to the fact that the request needs to be transmitted simultaneously to various countries on various continents, several common aspects need to be taken into consideration.

The first important issue is to identify the applicable treaty in each case and observe its provisions with regard to mutual legal assistance in general and the service of documents in particular. In most cases, the subpoenas cannot be submitted directly to the victims and consequently a mutual legal assistance request has to be formulated. When completing the request, one has to bear in mind that the subpoenas have to be submitted to the executing judicial authority with sufficient time before the actual term set for the trial. Moreover, one needs to know precisely whether the requested authority asks for the delivery of notification papers within a certain term, if it has special declarations in this sense. As one cannot assume that the domestic legislation of each State provides identical terms, the final term set for the trial needs to take into consideration all the conditions and deadlines provided by the laws of the requested States (some may provide for shorter terms and allow expedited means of communication, others may not). Therefore it will be highly probable that a longer term has to be established.

Another issue to be addressed relates to the content of the request. If certain countries have specific requirements on such content, the request submitted to those countries needs to be supported by relevant information. For example, in the case of common law countries, it may be needed to count the value of the harm done, as well as provide a detailed description of the facts of the case and a clear justification of the request.

One last issue to be addressed from the very beginning is the languages required for the subpoenas. In this case, the victims are located in many different countries and speak various languages. As nationals of the requested States, the subpoenas should be translated into a language the victims can understand.

In the case of countries A and B, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000) is applicable. Despite the fact that both States are parties to the Council of Europe Cybercrime Convention, the latter will not apply, as its provisions mainly confer priority to other treaties or bilateral agreements in force between the Member States (see Article 27(1) of the Cybercrime Convention)—in this case, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000.



### Article 5(2) of the 2000 EU MLA Convention

Procedural documents may be sent via the competent authorities of the requested Member State only if:

- (a) the address of the person for whom the document is intended is unknown or uncertain; or
- (b) the relevant procedural law of the requesting Member State requires proof of service of the document on the addressee, other than proof that can be obtained by post; or
- (c) it has not been possible to serve the document by post; or
- (d) the requesting Member State has justified reasons for considering that dispatch by post will be ineffective or is inappropriate.

[...]

In the situations mentioned in Article 5(2) due to the fact that the request will not be submitted directly to the addressee, a MLA request will need to be submitted to the authorities of the requested State which can be identified by using the European Judicial Atlas available at: [http://www.ejn-crimjust.europa.eu/atlas\\_advanced.aspx](http://www.ejn-crimjust.europa.eu/atlas_advanced.aspx) (depending on the requested State, it can be a judicial authority or a central authority). The notification papers need to be translated in the official language of country B (see Article 5(3)).

Between countries A and C, the Council of Europe Convention on Mutual Assistance in Criminal Matters (1959) is applicable. In this case, the transmittal is undertaken through central authorities. The documents that need to be served are accompanied by a MLA request. Many countries, when submitting the request, make use of forms that recall the general requirements of a MLA request stipulated by Article 14 of the 1959 Convention, which was presented in previous cases. The central authority from the requested State (in our case, country C) will forward the documents to the competent judicial authorities. The service of documents can be fulfilled by simple transmission or in a manner provided or compatible with the law of the requesting State.

### Article 7(1) of the CoE 1959 MLA Convention

[...]

Service may be effected by simple transmission of the writ or record to the person to be served. If the requesting Party expressly so requests, service shall be effected by the requested Party in the manner provided for the service of analogous documents under its own law or in a special manner consistent with such law.

In addition, it is important to check whether the two countries are parties to the Second Additional Protocol, 2001, which mentions in Article 16 that the service of documents may take place through post from the issuing judicial authority directly to the addressee (a provision similar to that stipulated in Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000).

## Second Additional Protocol of 8 November 2001 to the CoE MLA Convention 1959

### Article 16—Service by post

1. The competent judicial authorities of any Party may directly address, by post, procedural documents and judicial decisions, to persons who are in the territory of any other Party.

The notification papers need to be translated in the language of the executing state, addressing therefore the nationality of the victims.

Between countries A and D, A and E and A and G, the UNTOC will be applicable. The service of documents is mentioned *expressis verbis* in Article 18(3)(b) of the UNTOC as “effecting service of judicial documents”. As mentioned earlier regarding the Council of Europe 1959 Convention, the subpoena needs to be accompanied by a MLA request. Therefore, all the main issues that were discussed with regard to the application of the UNTOC on previous occasions will be of relevance, including the provisions of Article 18(15). With reference to the channels of communication, a direct contact with the victim by post, as provided for in the European Conventions, is not applicable. As a general rule, the contact should be done through central authorities.

The directory of competent national authorities is very practical for establishing the transmittal through central authorities or through diplomatic channels. Some of the countries involved may even accept the use of expedited means of communication, such as fax and e-mail. In this context, if there were no previous contacts, controlling the information provided for by the online directory could also be extremely useful.

In terms of the possibilities for country A to have contact with the countries in South America, the option allowed by the European Judicial Network (EJN)<sup>323</sup> should be considered. Country A, being an EU Member State and having contact points within EJN, can solicit the support of EJN in contacting<sup>324</sup> the relevant contact point of IberRed<sup>325</sup> (with the condition that the countries situated in South America are parties to the IberRed). This way of proceeding could prove extremely efficient when the request to notify the victim has an urgent character.

Between countries A and F there is an applicable bilateral treaty in force. The Council of Europe Cybercrime Convention would not have pre-eminence, due to the reasons outlined above (when describing the request transmitted from country A to B). The Convention could be invoked together with the bilateral instrument if the transmission of the documents has an urgent character and the use of the expedited means of communication provided for in Article 25 of the Convention is necessary or if referring to the mutual assistance regarding provisional measures such as data preservation alone (which is not the case here, taking into

<sup>323</sup> Information about the European Judicial Network can be found online at: <http://www.ejn-crimjust.europa.eu/>.

<sup>324</sup> EJN and IberRed are partners and each of the two regional networks can facilitate the contact of a member from the other network. The Memorandum of Understanding of the two networks can be found at: [http://www.ejn-crimjust.europa.eu/my\\_news/documents/MoU\\_EN.pdf](http://www.ejn-crimjust.europa.eu/my_news/documents/MoU_EN.pdf).

<sup>325</sup> IberRed is the abbreviation for Red Iberoamericana de Cooperación Jurídica Internacional, see *supra*, page 93. More information about the network of point of contacts can be found at <http://www.iberred.org/presentacion/>.

account the fact that we are speaking about a classical request of service of documents). The subpoenas can be transmitted through diplomatic channels or directly between the ministries of justice. Normally, in the case of a modern bilateral treaty the last hypothesis would be reasonable. Again, the use of fax or e-mail should be allowed as a general rule.

## 9. Ninth case—counterfeit documents/trafficking in persons

*Focus of the case:* Letter rogatory formulated during pre-trial phase. Organized crime component.

### *Facts of the case*

Offenders from country B are involved in an organized criminal group which is active in trafficking in minors for the purpose of sexual exploitation from country A to country C, using country B as a transit area. In order to assure the travel of minors to the destination country, they produce counterfeited documents that alter the age of the minors, so that they would appear as adults. Country B and C are parties to the Inter-American Convention on Mutual Assistance in Criminal Matters<sup>326</sup> (Nassau, 1992), but also parties to the UNTOC and the Trafficking in Persons Protocol (Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the UNTOC), while countries A and C are parties to the UNTOC and the Trafficking in Persons Protocol only. There is no bilateral treaty with regard to international cooperation applicable between countries C and B and countries C and A.

### *Object of the request*

The prosecutor from country C needs to forward requests to both countries A and B as follows:

- The request forwarded to country B refers to potential data about the criminal activity of the persons building the criminal group and, in case the offenders prove to have had previous criminal activities, data about them. In addition, in case there were reports, any kind of information or evidence already available to the judicial authorities from country B, the prosecutor from country C will ask for such data to be transmitted.
- The request forwarded to country A consists mainly in taking statements to various persons that were among the victims' entourage in country A. A second request will refer to the counterfeited documents, namely, if there were some known links between the investigated criminal organization with an organized criminal group in country A specialized in counterfeiting ID documents and other important elements that could help the investigation in country C. These data could already be in the possession of the judicial authorities of country A.

<sup>326</sup>The Convention is available online at: <http://www.oas.org/juridico/english/Treaties/a-55.html>.

## Strategy

### Informal contacts—transmission of the request

With regard to the request from country C to country B, it has to be stressed that before submitting the formal request, informal contacts through police channels should be used in order to get some initial elements about the organized criminal group and the elements held by the authorities from country B concerning its modus operandi. The Organization of American States (OAS), to which both countries are parties, recommends the use of alternative or collateral means of cooperation, due to the celerity of this type of cooperation:

It is recommended that Member States recognize the vital importance of other, less formal, methods of assistance, including the cooperation between the police forces of the respective Member States and that provision should be made for preserving and enhancing such direct cooperation to the extent possible.<sup>327</sup>

The formal request with the object underlined above will be transmitted on the basis of the Inter-American Convention on Mutual Legal Assistance in Criminal Matters (A-55), therefore the transmittal will be made from a central authority to a central authority.<sup>328</sup> A second possibility is to use the Hemispheric Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition<sup>329</sup> (the transmission of the MLA requests through central authorities does not preclude the judicial authorities of both countries from initial direct contacts, if the contact details of the executing judicial authority from country C are known).

Double criminality is not a precondition for executing the request, with some exceptions, which are prescribed in Article 5(2):

#### Article 5(2) of the Inter-American Convention on Mutual Assistance in Criminal Matters

When the request for assistance pertains to the following measures: (a) immobilization and sequestration of property and (b) searches and seizures, including house searches, the requested state may decline to render the assistance if the act that gives rise to the request is not punishable under its legislation.

When submitting the request, the forms mentioned earlier in the Proposed Best Practices could also be used.

<sup>327</sup> See, in this respect, the Proposed Best Practices with Respect to the Gathering of Statements, Documents and Physical Evidence, with Respect to the Mutual Legal Assistance in Relation to the Tracing, Restraint (Freezing) and Forfeiture (Confiscation) of Assets which are the Proceeds or Instrumentalities of Crime and Forms on Mutual Legal Assistance in Criminal Matters adopted in the Third Meeting of Central Authorities and Other Experts on Mutual Assistance in Criminal Matters and Extradition, Bogota, 12-14 September 2007, available at: [http://www.oas.org/juridico/MLA/en/best\\_pract\\_en.pdf](http://www.oas.org/juridico/MLA/en/best_pract_en.pdf).

<sup>328</sup> See, in this connection, Article 3, OAS MLA Convention.

<sup>329</sup> For more information about the Network, see: <http://www.oas.org/juridico/MLA/en/index.html>.

Referring to the request that needs to be forwarded from country C to country A, as previously stated, the UNTOC and the Trafficking in Persons Protocol<sup>330</sup> are applicable and need to be invoked together.

The formal request, particularly in relation to the counterfeited documents, could be preceded by informal cooperation between law enforcement agencies which is allowed by Articles 27 and 28 of the UNTOC and Article 10 of the Trafficking in Persons Protocol.

### Article 10 of the Trafficking in Persons Protocol

#### *Information exchange and training*

1. Law enforcement, immigration or other relevant authorities of States Parties shall, as appropriate, cooperate with one another by exchanging information, in accordance with their domestic law, to enable them to determine:

(a) Whether individuals crossing or attempting to cross an international border with travel documents belonging to other persons or without travel documents are perpetrators or victims of trafficking in persons;

(b) The types of travel document that individuals have used or attempted to use to cross an international border for the purpose of trafficking in persons; and

(c) The means and methods used by organized criminal groups for the purpose of trafficking in persons, including the recruitment and transportation of victims, routes and links between and among individuals and groups engaged in such trafficking, and possible measures for detecting them.

[...]

3. A State Party that receives information shall comply with any request by the State Party that transmitted the information that places restrictions on its use.

The comments made to the previous cases referring to the provisions of Article 18 of the UNTOC regarding the channels of communication, the use of the online directory of competent authorities or the printed version of this directory and the content of the request should be taken into account. In relation to the content of the request, the conditions provided for in Article 18(15) should be complied with.

### Execution of the request

The request shall be executed in accordance with the domestic law of the requested State. However, to the extent not contrary to the domestic law of the requested State and where possible, the request shall be executed in accordance with the procedures specified in the request (Article 18(7) of the UNTOC). Bearing in mind that one of the requests refers to taking statements from people knowing the victims, the requesting State needs to prepare a set of questions and a clear set of rules that need to be submitted to the requested State to ensure compliance with its procedure and allow the authorities from country C to use afterwards the evidence in court.

<sup>330</sup> The Trafficking in Persons Protocol can be found, together with UNTOC, at: <http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>, and the Legislative Guide at: <http://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html#traffickig>.

The fact that both countries are parties to the Trafficking in Persons Protocol facilitates not only the informal cooperation (see the above-mentioned Article 10, for example), but also the execution of the request to the widest extent possible (in this regard, see case 7 above referring to the smuggling of migrants and the reference made there to criminalization).

## 10. Tenth case—Joint Investigation Team (JIT)/trafficking of persons

*Focus of the case:* JIT formulated during the pre-trial phase, organized crime, bilateral and multilateral treaties applicable

### *Facts of the case*

An organized criminal group, acting from country A, is involved on a regular basis in trafficking in female teenagers (nationals of country A) to country B. In this context the organized criminal group uses falsified identification documents that indicate that the victims are adults. The victims are subsequently trafficked for the purpose of sexual exploitation in country B.

Countries A and B are on different continents. A bilateral treaty referring to mutual legal assistance in criminal matters and also the UNTOC are applicable.

### *Strategy*

In order to investigate the case, the investigative authorities from country B could establish a Joint Investigation Team (JIT) with authorities in country A. Indications for the use of such strategy are the complexity of the case and the transnational dimension. The JIT will be established in country B. Country A seconds this process by sending national experts to country B. The purpose of the JIT is to identify the victims, take their statements and gather information on the nexus of the criminal network based in country A.

The first step is the identification of applicable instruments. The bilateral treaty referring to mutual legal assistance should be invoked together with the UNTOC, which contains a provision on joint investigations (Article 19). Before entering into negotiations about JIT, it is generally recommended to send a MLA request asking for a preliminary agreement with regard to setting up a JIT first.

#### Article 19 of the UNTOC

States Parties shall consider concluding bilateral or multilateral agreements or arrangements whereby, in relation to matters that are the subject of investigations, prosecutions or judicial proceedings in one or more States, the competent authorities concerned may establish joint investigative bodies. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. The States Parties involved shall ensure that the sovereignty of the State Party in whose territory such investigation in whose territory such investigation is to take place is fully respected.

Once the preliminary agreement is reached, the JIT agreement between countries A and B needs to be set up. As previously mentioned, subject to the facts of the case, the establishment of an active integrated model<sup>331</sup> is recommended. In this context, several aspects need to be taken into account. The most important issues will be reminded here bearing in mind the models proposed by the Informal Expert Working Group on Joint Investigations,<sup>332</sup> as well as the recently adopted revised Model Agreement on the Establishment of a Joint Investigation Team.<sup>333</sup>

What JIT agreements need to comprise are, among other aspects, the parties of the agreement, the purpose of the JIT and the period covered, the JIT leader and the competence of the members and organizational arrangements.

- With regard to the parties of the agreement, countries A and B might have both competent authorities within prosecutors' offices and/or police. The agreement needs to define the competent authorities involved.
- The purpose of the JIT has to be clearly defined. In the particular case, the JIT is established in order to disrupt a criminal network involved in trafficking of human beings (THB) by identifying the victims and taking the victims' statements. The team needs to undertake investigative measures in order to identify the victims and to reveal information about the offenders. The involvement of national experts from country A that have the victims' nationality could be a significant advantage.
- It is important to define the period of time necessary for the JIT to operate. If the investigations face unforeseen difficulties the need for an extension of the period of time can be evaluated during follow up procedures.
- The JIT leader has to be established among the representatives of country B (host country) bearing in mind the fact that the type of JIT established is an active integrated model.
- With regard to the competences of the participants of the JIT, potential difficulties might occur with seconded national experts. They need to be clearly defined in the agreement, taking into account the fact that the seconded national experts will not have a mere consultative role but will participate in the actual investigation. In this context, the JIT leader or another member of the JIT needs to train the seconded experts to ensure that, for example, evidence is collected in line with the rules and procedures of the host country (country B). This is especially relevant in those cases where representatives from a country with different legal systems are involved (civil law/common law).
- With regard to organizational arrangements, it is recommended to bear in mind the coverage of costs of personnel (e.g. travel expenses, daily expenses for seconded members), as well as the costs of the investigative measures per se (usually these are covered by the host country). The JIT agreement could also include regulations

<sup>331</sup> For the classification, see the Report of the Informal Expert Group on Joint Investigations, Conclusions and Recommendations, 2-4 September 2008, Vienna.

<sup>332</sup> Ibid.

<sup>333</sup> The revised Model Agreement was adopted by Council Resolution of 26 February 2010(2010/C70/01), available online at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:070:0001:0012:EN:PDF>.

related to confidentiality as well as the involvement of regional networks and organizations (at the EU level especially Eurojust and EUROPOL could be included).

- The main competences of the seconded representatives as well as their obligations should also be clearly defined. With regard to the conditions of the agreement, a good example of possible conditions can be found in Article 13(3) of the EU Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union (2000).

#### Article 13 OF THE 2000 EU MLA Convention

3. A joint investigation team shall operate in the territory of the Member States setting up the team under the following general conditions:

- (a) The leader of the team shall be a representative of the competent authority participating in criminal investigations from the Member State in which the team operates. The leader of the team shall act within the limits of his or her competence under national law;
- (b) The team shall carry out its operations in accordance with the law of the Member State in which it operates. The members of the team shall carry out their tasks under the leadership of the person referred to in subparagraph (a), taking into account the conditions set by their own authorities in the agreement on setting up the team;
- (c) The Member State in which the team operates shall make the necessary organizational arrangements for it to do so.

## 11. Eleventh case—Internet-related offence

*Focus of the case:* Application of Internet-specific investigation instruments

### *Facts of the case*

An offender in country A is setting up a spoofed website that looks like the website of a legitimate financial institution registered in and operating from country B. The website is hosted by an Internet provider in country A. A number of Internet users located in country B access the website and disclose identity-related information. That information is then used to access the victim's bank account and initiate transfer processes. Country A and country B have ratified the Council of Europe Convention on Cybercrime.

### *Background information*

Identity-related offences committed by using means of network technology are a growing concern. “Phishing” and account takeover are just two keywords used to describe typical Internet-related phenomena. In general, the main concern in this regard is not the missing criminalization of Internet-related offences but challenges related to the investigation.



The identification of an offender who has committed a cybercrime may require the analysis of traffic data.<sup>334</sup> Information that is relevant for the identification is often deleted shortly after they are not required anymore for the procession of data transfer processes.<sup>335</sup> A very short response time by the investigative authorities is often vital for a successful investigation. Without adequate legislation and instruments allowing investigators to act immediately and prevent data from being deleted, an effective fight against cybercrime may not be possible.<sup>336</sup>

### Strategy

Even if means of expedited communication are used, international cooperation is in general a time-consuming process. This is especially relevant when comparing it to the speed of data transfer and automatic deletion processes. The focus of the strategy therefore needs to be on the preservation of data. In the present case, the log-files generated by the hosting provider are of particular interest. As both countries ratified<sup>337</sup> the Council of Europe Convention on Cybercrime, a procedural instrument that enables law enforcement to order the expedited preservation of computer data is available on the national level.

#### Article 16 of the 2001 CoE Convention on Cybercrime

##### *Expedited preservation of stored computer data*

- (1) Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
- (2) Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
- (3) Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
- (4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

<sup>334</sup>“Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required”, see Explanatory Report to the Council of Europe Convention on Cybercrime No. 155, supra n. 159; Regarding the identification of suspects by IP-based investigations, see Gercke, Preservation of User Data, Datenschutz und Datensicherheit, 2002, page 577 et seq.

<sup>335</sup>Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, 2002. available at: <http://www.citeulike.org/user/alexbdigital/article/80546>.

<sup>336</sup>Regarding the necessary instruments, see Gercke, Understanding Cybercrime..., supra n. 26, chapter 6.2. One solution that is intensively discussed is data retention. Regarding the possibilities and risks of data retention, see Allisch, Data Retention on the Internet—A measure with one foot offside?, *Computer Law Review International* 2002, page 161 et seq.

<sup>337</sup>A full list of countries that signed and ratified the Council of Europe Convention on Cybercrime (ETS 185) is available at: <http://www.conventions.coe.int>.

As the fundamental principle of national sovereignty limits the ability to carry out investigations outside the territory, Country B can not simply use this instrument to oblige the hosting provider to preserve the stored computer data.

### Practical advice

The only provision in the Convention that would allow a direct interaction between law enforcement authorities in country B and the service provider registered and operating in country A is Article 32(b) of the Convention on Cybercrime. It allows law enforcement to access computer data (such as log-file information) stored outside their territory if the investigators have obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data. This authorisation is heavily criticized.<sup>338</sup> There are good arguments against such regulation. The most important one is the fact that by establishing the second exemption, the drafters of the Convention are violating the dogmatic structure of the mutual legal assistance regime in the Convention.<sup>339</sup>

Instead, country B needs to refer to the procedures defined by Article 29 of the Convention on Cybercrime.

### Article 29. Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2. A request for preservation made under paragraph 1 shall specify:
  - (a) the authority seeking the preservation;
  - (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
  - (c) the stored computer data to be preserved and its relationship to the offence;
  - (d) any available information identifying the custodian of the stored computer data or the location of the computer system;
  - (e) the necessity of the preservation; and
  - (f) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

[...]

<sup>338</sup> Report of the Second Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2, available at: [http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20\(2007\)%2003%20E.pdf](http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2007)%2003%20E.pdf).

<sup>339</sup> For more details, see *Gercke, Understanding Cybercrime...*, supra n. 26, chapter 6.3.

### Practical advice

In light of the urgency of the request, the use of the 24/7 network should be taken into consideration. In order to improve the efficiency of mutual assistance requests, the Convention obliges States parties to designate a contact point for the mutual assistance requests that is available without time limitations.<sup>340</sup> As both countries in the case example signed and ratified the Convention they need to have such a contact point in place. The drafters of the Convention emphasized that the establishment of the points of contact is one of the most important instruments provided by the Convention on Cybercrime.<sup>341</sup> A checklist of requests for expedited preservation of computer data sent through 24/7 networks can be found in the discussion paper “The Functioning of 24/7 Points of Contact for Cybercrime”, Council of Europe, 2009, available at: <http://www.coe.int/cybercrime/>.

Article 29 provides for a mechanism at the international level equivalent to that provided for in Article 16 for use at the domestic level. While much more rapid than ordinary mutual assistance practice, this mechanism is at the same time less intrusive. The mutual assistance officials of the requested Party are not required to obtain possession of the data from its custodian. The preferred procedure is for the requested Party to ensure that the custodian (frequently a service provider or other third party) preserve (i.e., not delete) the data pending the issuance of process requiring it to be turned over to law enforcement officials at a later stage. This procedure has the advantage of being both rapid and protective of the privacy of the person whom the data concerns, as it will not be disclosed to or examined by any government official until the criteria for full disclosure pursuant to normal mutual assistance regimes have been fulfilled. At the same time, a requested Party is permitted to use other procedures for ensuring the rapid preservation of data, including the expedited issuance and execution of a production order or search warrant for the data. The key requirement is to have an extremely rapid process in place to prevent the data from being irretrievably lost.<sup>342</sup>

<sup>340</sup>The availability 24 hours a day and 7 days a week is especially important with regard to international dimension of Cybercrime, as requests can potentially come from any time zone in the world.

<sup>341</sup>See Explanatory Report to the Convention on Cybercrime, supra n. 157, paragraph 298.

<sup>342</sup>Ibid, paragraph 283.



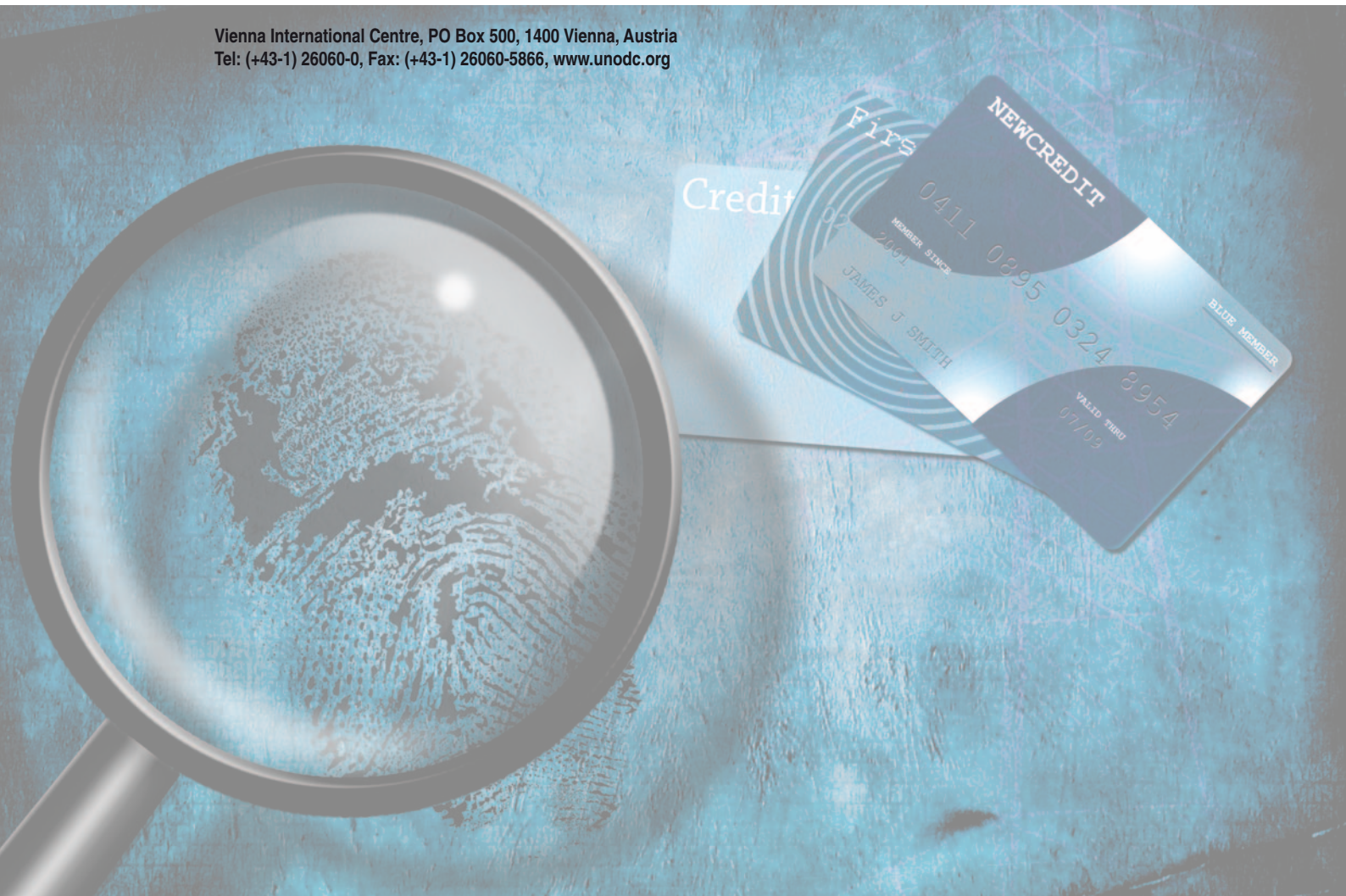




# UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria  
Tel: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, [www.unodc.org](http://www.unodc.org)



Printed in Austria



V.10-58702—April 2011—1,500