15 April 2009
English only

Commission on Crime Prevention and Criminal Justice
Eighteenth session
Vienna, 16-24 April 2009
Item 3 (a) of the provisional agenda*
Thematic discussion: "Economic fraud and identity-related crime"

IDENTITY-RELATED CRIME VICTIM ISSUES: A DISCUSSION PAPER

Philippa Lawson[1]

February 2009

* E/CN.15/2009/1 and Corr.1.

[1] 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. The opinions expressed in this paper are those of the author and do not reflect the views of the United Nations.

V.09-82606 (E)

Contents

Identity-Related Crime Victim Issues: A Discussion Paper

Philippa Lawson[2]
February 2009

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:

1) The range and types of victims of identity-related crime;

2) Legal bases for victim remediation, including an analysis of rights to identity, reputation and privacy; and

3) An Inventory of State and private sector practices for victim support and remediation.

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,[3] "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.

---

[2] M.A., LL.B., Barrister & Solicitor, Ontario, Canada.
[3] E/CN.15/2007/8.

PART I: RANGE AND TYPES OF IDENTITY-RELATED CRIME VICTIMS

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.[4] 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 US, 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 US survey, 5% of Americans were victims of identity-related crime in 2006, an over 50% increase since 2003.[5] In Canada, one 2008 survey found that "about 1 in 10 Canadians reports having been a victim of identity theft",[6] while another 2008 survey found that 6.5% 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.[7] A recent study in the UK found a 66% increase in identity fraud victims contacting the national credit reporting agency in 2007

---

4 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.

5 Gartner Inc., Press Release (March 6, 2007).

6 EKOS Research Associates, quoted in Criminal Intelligence Service Canada, *Annual Report 2008*,"Feature Focus: Identity Theft and Identity Fraud in Canada".

7 Sproule and Archer, *Measuring Identity Theft in Canada: 2008 Consumer Survey*, MeRC Working Paper #23 (July 2008) ["Sproule and Archer"].

versus 2006,[8] and an almost 50% increase in the first half of 2008 over the same period in 2007.[9] The UK financial industry also reported high rates of growth of economic identity fraud – over 200% for account takeovers – in 2008.[10]

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.[11] 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.[12]

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.[13] A recent study by Javelin Research in the US 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. In addition, a 14-year-old had a more than $600,000 mortgage in his name and the house later went into foreclosure.[14]

In the US, complaint-based statistics suggest that individuals in the 18-29 year age range are most likely to be victims of identity-related crime generally, and that the rate of

---

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

9 Experian UK, News Release (October 8, 2008).

10 CIFAS, Press Release: "2008 Fraud Trends"(January 26, 2009).

11 FIDIS, "D12.7: Identity-related crime in Europe – Big Problem or Big Hype?" (June 9, 2008) ["FIDIS"], p.62.

12 Bi-national Working Group on Cross-Border Mass Marketing Fraud (Canada-US), *Report on Identity Theft* (October 2004).

13 Steven Malanga, "Identity Theft in America goes Hand and Hand with Illegal Immigration"; online at <http://www.usbc.org/opinion/2008/spring/identity.htm>.

14 Javelin Strategy and Research, News Release: "Recent Javelin Study Shows Children Are At Risk for Identity Theft" (October 28, 2008).

victimization decreases with age (unlike many other forms of fraud for which the elderly are prime targets).[15] 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.[16] A UK 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.[17]

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."[18]

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."[19]

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.[20]

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

---

15 FTC, *Consumer Fraud and Identity Theft Complaint Data*, January – December 2007, p.15.

16 Criminal Intelligence Service Canada, *Annual Report 2008*, "Feature Focus: Identity Theft and Identity Fraud in Canada".

17 Home Office Statistical Bulletin, *Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey* (May 15, 2007), p.35.

18 Experian UK, Press Release (October 8, 2008).

19 Australian National Crime Prevention Program, *Identity Theft Information Kit* (May, 2004), online at <http://www.crimereduction.homeoffice.gov.uk/theft1.htm>.

20 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, (Nov.3, 2008), http://www.ehip.ca; reported in Pauline Tam, "ID theft Scams Target Canada's Healthcare System", *The Ottawa Citizen* (Nov.3, 2008).

"synthetic" identity fraud accounts for half of all identity fraud in the US.[21] 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 US, 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.[22]

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.

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.[23]

The US Federal Trade Commission ("FTC") separates identity-related crime (which it calls "identity theft") into four categories: "existing credit card accounts", "existing non-credit card accounts", "new accounts", and "other". This categorization reflects current incidence levels in the US. 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

---

[21] Allen Jost, Vice-President, Business Strategy, ID Analytics; telephone interview (February 3, 2009).

[22] See Leslie McFadden, "Detecting Synthetic Identity Fraud", www.bankrate.com (May 16, 2007).

[23] Synovate, Figure 2, p.13; Identity Theft Resource Center, *Identity Theft: The Aftermath 2007*, ["ITRC, *Aftermath*"] Tables 1A and 1B.

detection by authorities, such as illegal immigrants, drug couriers and criminals engaged in money-laundering.[24]

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 UK 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).[25] 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 UK Fraud Prevention Service, reports significant increases in fraudulent use of existing accounts, distinguishing between "account takeover", for which there was a 207% increase in 2008 over 2007, and "account misuse", for which there was a 69% increase over the same period.[26]

---

[24] UK Cabinet Office, *Identity Fraud: A Study* (July 2002).

[25] ITRC, *Aftermath*, Tables 1A and 1B.; European Fraud Prevention Expert Group, *Report on Identity Theft/Fraud* (October 22, 2007) ["FPEG"], pp.8-9.

[26] CIFAS, Press Release: *2008 Fraud Trends* (January 26, 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 UK For the most part, the direct costs of such fraud are borne not by the individual victim but by credit card companies,[27] 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 reparable 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.[28] In the US, consumers are protected by law from liability for unauthorized electronic fund transfers depending upon the timing of consumer notice to the applicable financial institution.[29]

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 US. 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' licences, 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, UK citizens have been contacted by the police to answer for

---

[27] For example, the US *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.

[28] See, for example, the UK *Banking Code* (March 2008), ss.12.11 – 12.13, online at http://www.bba.org.uk/content/1/c6/01/30/85/Banking_Code_2008.pdf.

[29] *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).

crimes allegedly committed by a child of theirs who died in infancy.[30] Counterfeit documents are also frequently used to access services.

Identity-related tax fraud

This form of identity fraud has increased dramatically in the US 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.[31] 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 US taxpayer was reportedly faced with a $1m. 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.[32]

Medical identity fraud

Healthcare fraud is a particular concern in the US, where universal health insurance is not provided by the State.[33] 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.[34]

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' licence 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 licence. 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 licence because outstanding fines

---

30 UK Cabinet Office, *Identity Fraud: A Study* (July, 2002), para.1.2.

31 Federal Trade Commission, *Consumer Fraud and Identity Theft Complaint Data, January – December 2007* ["FTC, 2007 Complaint Data"].

32 Kevin McCoy, "Identity thieves tax the system", *USA Today* (April 10, 2008).

33 http://www.worldprivacyforum.org/medicalidentitytheft.html.

34 Max Alexander, "Your Medical Records, Stolen!", *ReadersDigest.com.*

must be paid before they will be allowed to renew insurance or a driver's licence".[35] Identity criminals also use drivers' licence information to engage in other fraudulent activity, taking advantage of widespread use of drivers' licences for authentication purposes.

But even where it does not involve impersonation of live victims, drivers licence fraud creates public safety risks and significant costs to the public treasury. In the UK, it is estimated that detection and investigation of identity fraud in drivers' licence application and testing processes cost the government £7m. per year.[36]

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.[37] 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.[38] Real estate fraud is now a serious issue in Canada, and tops the US Identity Theft Resource Center's list of predictions for 2009.[39]

Employment Fraud

The US has seen a marked increase in employment fraud in recent years, with criminals impersonating US 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.[40] 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

---

35 British Columbia Crime Prevention Association, "Identity Theft Victim's Toolkit" (February 2007).

36 UK Identity Fraud Steering Committee, "New Estimate of Cost of Identity Fraud to UK Economy" (October 9, 2008).

37 Law Society of Upper Canada, Report to Convocation, *Mortgage Fraud (*March 24, 2005).

38 Dale Anne Freed, "Mortgage Fraud Victory; Woman wins back home as court reverses decision", *The Toronto Star* (Feb.7, 2007).

39 *Ibid;* "Mortgage fraud hits $1.5b. per year", *Calgary Herald* (March 18, 2006); Identity Theft Resource Center, Press Release "Identity Theft Predictions 2009" (December 18, 2008).

40 FTC, 2007 Complaint Data.

that they never committed. For example, a US 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.[41]

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.

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 though methods and from sources such as the following:

- finding lost wallet, account/password information
- sifting through trash
- theft: stealing wallet, chequebook, credit card, mail[42]
- eavesdropping on insecure wireless communications[43]
- personal websites
- social networking sites[44]

---

41 Reported on KVBC TV, Las Vegas NV (May 13, 2008), accessed January 31, 2009 on www.youridentitysafe.com.

42 There may be little that a victim could have done to prevent theft.

43 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.

44 Social networking sites bear some responsibility for warning users, especially young people, of the risks entailed with posting personal information on the site.

Victim deception:

In many cases, victims are tricked into providing their data, either directly to the fraudster or via surreptitious computer programs 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, email ("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"[45]

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 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

[45] Embedding concealed links that execute without the user's knowledge when the user clicks on visible links on a webpage.

- hacking into computer systems/databases
- taking advantage of security breaches

By nature of damage suffered[46]

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 programs 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 US survey estimates that identity-related crime cost individual victims an average of $691 (with more than half incurring no expenses) in 2007,[47] while a 2006 survey commissioned by the FTC found that 10 percent of identity crime victims reported out-of-pocket expenses of $1,200 or more, and the top 5 percent incurred expenses of at least $5,000.[48] A third US 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 percent in 2005 to 61 percent in 2006.[49] Victims who contacted the US 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.[50]

According to a recent Canadian survey, victims of identity-related crime spent a total of over $155m.to resolve problems associated with the crime, with a mean cost per victim of $92, or $151 excluding credit card fraud.[51]

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

---

46 For the purposes of this typology, we look at organizations (public and private) as well as individual victims.

47 Javelin Strategy and Research, News Release: "Identity Fraud, Part 1: A $45 Billion Snowball" (September 27, 2008).

48 Synovate, *2006 Identity Theft Survey Report*, prepared for the Federal Trade Commission (November 2007) ["Synovate"], p.6.

49 Gartner, News Release (March 6, 2007).

50 ITRC, *Aftermath*, Executive Summary.

51 Sproule and Archer, p.17.

damage or time taken off work).[52] A significant number of victims in the US report difficulties getting credit agencies to remove inaccurate information from their files, or stopping them from putting negative information back in their records.[53]

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' licences, 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 UK 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.[54]

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 healthcare 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.[55]

Wrongful detention/arrest

Many US citizens have been arrested for crimes committed by others who successfully impersonated them using stolen identity information. An alarming 62% of respondents to a recent survey of victims by the US Identity Theft Resource Center reported that criminals had committed financial crimes resulting in warrants being issued in the victim's name – more than 2 ½ times higher than in 2006 and double the amount from 2004.[56]

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 US Identity Theft Resource Center's 2007 victim survey, 82% 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 US Identity Theft Resource Center's

---

52 Synovate, p.7.

53 ITRC, *Aftermath*, Executive Summary.

54 Marc Sigsworth, "I was falsely branded a paedophile", BBC News online, 2008/04/03.

55 As noted above, there is evidence of US citizens fraudulently accessing the Canadian healthcare system using the identities of deceased Canadians.

56 ITRC, *Aftermath*, Executive Summary.

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. Mean resolution time per victim, according to a 2007 survey, was 40 hours.[57] A Canadian survey estimates that victims there spent a total of 21m. hours restoring their identity information, 13 hours on average per victim, and 17 hours when credit card fraud is excluded.[58] Victims who contacted the US 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% of cases, one to two years in 12% of cases, and two or more years in 19% of reported cases.[59]

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.[60] 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".[61]

"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."[62]

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."[63] 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

---

57 Javelin Strategy and Research, News Release: "Though national statistics are trending downward, millions of Americans still at risk for identity theft" (October 8, 2008).

58 Sproule and Archer, p.17.

59 ITRC, *Aftermath*, Executive Summary.

60 See ITRC, *Aftermath*, pp.26-29: "Emotional Impact on Victims".

61 Dr. Charles Nelson, quoted in ITRC, *Aftermath*, p.27.

62 Jessica Van Vliet, quoted in Karen Kleiss, "'Woman had her bank accounts drained, found herself under investigation for fraud", *The Edmonton Journal*, December 20, 2008.

63 ITRC, *Aftermath*, p.31.

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."[64] 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."[65]

Businesses

Victims of corporate identity theft/fraud and corporations that are defrauded by criminals posing as others suffer a variety of kinds of damage, including:

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 US Identity Theft Resource Centre in 2007 reported average losses of almost $50,000.[66]

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).

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.

---

64 Licia Corbella, "I.D. theft hits home", *Calgary Sun* (November 23, 2007).

65 ITRC, *Aftermath*, p.31.

66 *Ibid*., highlights.

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

Damages incurred by governments as a result of identity-related crime include:

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' licence, 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 ID-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 US 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.[67] 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.[68]

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.[69]

---

67 ITRC, *Aftermath*, Table 7, pp.14-15; Sproule and Archer, pp.22-23.

68 Synovate, p.28, Figure 9; Sproule and Archer, pp.22-23.

69 Sproule and Archer, p.23.

PART II: 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.

Normative Basis for Victim Remediation: Victims' Rights Initiatives

UN 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*.[70] 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.
>
> …
>
> 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:

[70] G.A. Resolution 40/34, (November 29, 1985). Work is currently underway on a draft UN 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.

(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 UN Declaration is of little assistance.

Nevertheless, the UN 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 UN Declaration, many States have taken measures to assist victims of crime, including the enactment of victims' rights laws.[71] 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).[72]

Non-legislated Principles, similar to those in the UN 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,

[71] E,g, New Zealand, *Victims' Rights Act, 2002.*

[72] 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).

about the progress of the investigation and prosecution; and should have their views and concerns taken into consideration by investigators and prosecutors.[73]

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.[74] Given the narrow focus of these regimes on violent crime, it is unlikely that victims of identity-related crime would qualify for such compensation.

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.[75] 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*[76] ("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.

---

[73] *Ibid.*

[74] Blindell, *op cit.* See also legislative regimes for criminal injuries compensation in Canada and the US.

[75] International Victimology Institute, Tilburg University ("INTERVICT"), see 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".

[76] G.A. resolution 55/25 (November 15, 2000).

Both the Palermo Convention and the *United Nations Convention Against Corruption*[77]("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.[78] The Palermo Convention also requires that State Parties develop or improve specific training programs dealing among other things with "methods used in the protection of victims and witnesses".[79]

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.

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.[80]

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

---

77 G.A. resolution 58/4 (October 31, 2003).

78 Palermo Convention, Article 14(2); Merida Convention, Article 57(3)(c).

79 Article 29(1)(i).

80 E.g., *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.[81] 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 US, 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."[82]

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.[83] 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)[84]
- Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)[85]

---

81 Such legislation also appears in the inventory of public sector practices for victim remediation, below.

82 Directive 2002/65/EC, Article 8.

83 Electronic Privacy Information Centre and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007). ["EPIC et al"]

84 See www.oecd.org.

- UN Guidelines Concerning Computerized Personal Data Files (1990)[86]
- 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)[87]
- Asia Pacific Economic Cooperation (APEC) Privacy Framework (2004)[88]

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.[89] 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)

---

85 Council of Europe Convention No.108 (18 Sept 1980).

86 Adopted by General Assembly Resolution 45/95 (December 14, 1990).

87 Directive 95/46/EC.

88 APEC Privacy Framework (2005).

89 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.

- *Individual Participation* (individuals should have rights to access data about them held by the data controller and to have inaccurate data corrected)

- *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.[90]

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.

---

[90] 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.* (Sept.25, 2007).

Security measures also include *effective authentication* of those making requests for data or applying for services such as credit. Failure to properly authenticate applicants 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.[91]

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.[92] Under other models, they must apply to the court for compensation or other enforceable remedies.[93] 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.

---

[91] 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).

[92] E.g., private sector data protection statutes in the provinces of Quebec, Alberta and British Columbia, Canada.

[93] This is the case under Canada's federal private sector law, the *Personal Information Protection and Electronic Documents Act*.

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 sector.[94] Many civil codes, for example, provide for an actionable right to privacy.[95] 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.[96]

Such actions are also possible under the *tort of "misappropriation of personality"* recognized by some common law courts.[97] 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 identity 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.[98] This cause of action treats intrusion into one's seclusion, solitude or private affairs as a civil wrong for which damages may be awarded.

---

94 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.

95 For example, the French Civil Code, Articles 9 and 1382; Civil Code of Quebec, S.Q., 1991, c. 64, Articles 35, 36.

96 *Aubry v. Editions Vice-Versa Inc.*, [1998]1.S.C.R. 591.

97 See, for example, *Horton v. Tim Donut Ltd.* (1997), 75 C.P.R. (3d) 467 (Ont.C.A.).

98 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.).

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 program for related costs.[99]

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 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

[99] See FIDIS, p.40.

reporting by a credit bureau, is found to constitute libel insofar as it causes harm to the victim's reputation.[100] 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 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.[101]

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.[102] 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.[103]

In the US, 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

---

100 We have found no case law or authoritative commentary on this.

101 Microsoft, for example, has claimed trademark infringement in a number of lawsuits against people fraudulently posing as Microsoft in email phishing scams. See for example Todd Bishop, "Microsoft casts net for phish culprits", *Seattle Post-Intelligencer* (April 1, 2005).

102 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.

103 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.

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.[104]

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 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).[105] 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.

---

[104] See Jeffrey Dion and James Ferguson, "Civil Liability for Identity theft", (Feb 1, 2007); online at 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), online at http://www.jenner.com/files/tbl_s20Publications/RelatedDocumentsPDFs1252/380/Identity_Theft.pdf.

[105] Jennifer Chandler, "Negligence Liability for Breaches of Data Security", 23 *Banking & Finance Law Review* (2008), 223-247.

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."[106]

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.

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.[107] In some jurisdictions, constitutional rights may apply directly to the private sector.[108]

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 "drittworkung", 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")[109] 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,[110] 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

---

106 Blindell, (2006).

107 See Dawn Oliver and Jörg Fedtke, eds., *Human Rights and the Private Sphere: A Comparative Study* (Routledge, 2007).

108 For example, Article 25(1) of the Greek Constitution states: "These rights also apply to the relationship between individuals wherever appropriate."

109 i.e., the right to respect for private and family life. See below, under "Right to Privacy" for a substantive discussion of this right.

110 *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.

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).

…

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).[111]

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.

[111] *K.U. v. Finland*, Appl. No. 2872/02 (December 2, 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.

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 programs 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.[112] 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.");
- *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

[112] 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 (April 16, 2007).

citizens can enjoy basic rights.[113] 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 *UN Declaration on the Protection of All Persons from Enforced Disappearance*,[114] Art.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 *UN Convention on the Rights of the Child*, Art.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."

Application to Identity-Related Crime

The right to identity has not been widely promoted (if at all) as the basis for programs 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.

---

113 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 (May 15, 2007).

114 G.A.Res. 47/133, UN GAOR, 47th Sess., Supp. No. 49, art. 20, UN Doc. A/47/49 (1992).

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.[115]

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 *UN 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:

---

[115] *X v. Iceland*, 5 Eur. Comm'n H.R. 86.87 (1976).

> "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 of privacy in some form, 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.[116] Most recently written constitutions include specific rights to access and control one's personal information.[117]

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.[118]

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 *drittworkung* in Europe. In a ECHR case noted above,[119] 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

---

116 Sections 7 and 8.

117 EPIC et al.

118 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.*

119 *X and Y v. The Netherlands, op cit.*

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 programs and actions to assist victims of identity-related crime. Under the European *drittworkung* 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.

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.[120]

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."[121]

[120] Council of Europe, *Convention on Cybercrime,* CETS No.185.

[121] Draft Convention, online at <http://www.tilburguniversity.nl/intervict/undeclaration/convention.pdf>.

PART III: 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 US than in other countries.[122] 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.

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 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.

[122] 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).

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 identity 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 US 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.[123] 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 US Dept. of Justice ("DOJ") Criminal Division, US Attorneys' Offices, the FBI, the Department of the Treasury, the FTC, the Diplomatic Security Service, the US Secret Service, and the US 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 US 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;

[123] See website of President's Task Force on Identity Theft: http://www.idtheft.gov.

- The US "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 US 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.[124]

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 UK "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.[125]

- 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 email address for reporting and obtaining assistance with this particular problem;

- "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 US 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

[124] http://www.recol.ca.

[125] See <http://www.identity-theft.org.uk/committee.asp>.

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.[126]

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.[127] 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*;[128]

- 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;[129]

- 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;[130]

---

126 See http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html.

127 See OECD, Directorate for Science, Technology and Industry, Committee on Consumer Policy, *Scoping Paper on Online Identity Theft*, DSTI/CP(2007)3/FINAL (February 19, 2008) ["OECD"], pp.45-55 for a more comprehensive list and description of such initiatives.

128 E/RES/2007/20 (July 26, 2007); see also E/RES/2004/26 (July 21, 2004).

129 See OECD, *op cit*, pp.45-46.

130 As reported in OECD, *op cit*.

- The "London Action Plan", a global network of public and private sector parties focused on cooperating internationally to combat spam;[131]

- 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.[132]

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 US *Identity Theft and Assumption Deterrence Act 1998,* which created a specific offence of "identity theft",[133] the Federal Trade Commission ("FTC") was tasked with creating a central information, assistance and complaint-referral service for victims of identity-related crime.[134] 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 US 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.

---

131 *Ibid.*; a major technique used by identity criminals to gather personal data from victims is "phishing", i.e., the use of unsolicited bulk email ("spam") to deceive individuals into providing their account and other data.

132 *Ibid.*

133 Defined broadly to include identity fraud and related acts: 18 USC. § 1028.

134 Pub. L. No. 105-318 § 5, 112 Stat. 3010 (1998).

Expand existing programs for victims of crime to cover identity-related crime

Many States have services and programs designed specifically to assist, support and/or compensate victims of crime. Such programs tend to focus on victims of violent crime or other crimes fundamentally different in nature from identity-related crime, and are not 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 US 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.[135]

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.[136]

Support private sector victim support initiatives/programs

Victim support can often be provided more effectively by non-governmental agencies devoted to the issue. In the US, where identity-related crime appears to be most prevalent, there are a number of such organizations. In 2007, the US government awarded $1.7m.through its Office for Victims of Crime to existing national, regional, state and local victim service organizations for the purpose of supporting programs that assist victims of identity-related crime.[137]

The US Dept of Justice ("DOJ") is currently collaborating with the American Bar Association to set up a program 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.

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

135 http://www.ojp.gov/ovc/publications/infores/focuson2005/identitytheft/welcome.html

136 *Victims' Rights Act 2002* (N.Z.) 2002/39.

137 See press release at: http://www.ojp.usdoj.gov/newsroom/pressreleases/2007/OVC08006.htm.

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 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 US Office for Victims of Crime runs courses specifically aimed at training law enforcement and victim assistance counsellors to manage identity-related crime.[138]

The FTC and other US 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.[139]

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.[140]

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 US *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 (1) in clearing the credit history or credit rating of the victim; or (2) 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."[141] Similar amendments to the Canadian Criminal Code have been proposed to permit restitution to victims of identity crimes.[142]

---

138 See, for example, http://www.sei2003.com/ovcttac2008/SanDiego-Identitytheft.htm, http://www.ovcttac.gov/trainingCenter/workshop_descriptions.cfm#WS5.

139 The President's Identity Theft Task Force, "Combating Identity theft - Volume II", part O.

140 "The President's Identity theft Task Force Report" <http://www.idtheft.gov/reports/IDTReport2008.pdf>. at p. 26.

141 18 USC. 3663A(c)(1)(A).

142 Bill C-27, introduced in the 39th Parliament.

The recently enacted US *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."[143] This is important given the amount of time that victims of identity-related crime typically must spend restoring their identity information and reputation.

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",[144] 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,

[143] 18 USC. 3663(b).

[144] www.restorativejustice.org.

saying that it would not compensate scam victims unless they could prove that the bank was at fault.[145]

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. 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 Program, 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.[146]

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 UK, public and private sector organizations have partnered to create the website www.identity-theft.org.uk, a central repository of information on identity-related crime.[147] Australia has also created a central website for information for victims and others on identity-related crime.[148] In the US, the FTC has operated such a site for some years,[149] and 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 US.

The International Association of Chiefs of Police has partnered with the Bank of America to publish the website 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.

---

145 See "Korean Banks forced to compensate hacking victims", *Finextra.com* (December, 2005); online at <http://www.finextra.com/fullstory.asp?id=14634>.

146 See link to "ID Theft Kit" on <http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity#q3>.

147 http://www.identity-theft.org.uk/.

148 http://www.stopidtheft.com.au/.

149 See http://www.ftc.gov/bcp/edu/microsites/idtheft/.

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,[150] and general crime victim resource centres such as those in Maryland, US[151] and the Netherlands.[152]

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 US FTC publishes on its website an "Identity Theft Victims' Statement of Rights", summarizing victims' rights in the US.[153] 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 US 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*.

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.[154] 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.

---

150 See: http://www.idvictim.org/AboutUs.cfm?pagename=AboutUs for a more detailed description of their mission and services.

151 See: http://www.mdcrimevictims.org/_pages/id_theft.html.

152 See: http://www.slachtofferhulp.nl/.

153 See http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/rights.html for the complete list.

154 http://www.phonebusters.com/images/IDtheftStatement.pdf.

In addition to educating law enforcement agencies about the importance of providing such reports, US 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.[155]

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.[156]

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 US states have passed security breach notification laws requiring that organizations notify individuals of breaches that expose their data to potential identity-related crime.[157] 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.

---

155 See http://www.ftc.gov/bcp/edu/microsites/idtheft/tools.html.

156 http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-expunge.html provides a list of all of the states with such a law, as well as a link to the relevant statute.

157 See: http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

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, restore credit, and prevent further misuse of their personal information. The program also prevents duplicate entries of the victim's information.[158] A number of other US states have since begun similar programs.[159]

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 US, a whole new industry is developing to serve victims of identity-related crime.[160] 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.

---

158 See: http://www.ag.state.oh.us/victim/idtheft/index.asp.

159 http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-passport.html provides a link of the states with a passport type program as well as links to the statutes.

160 See, for example, prepaidlegal.com, trustedID.com, myidesite.com, creditfyi.com, idcure.com, identitytheft911.com, myidfix.com.

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.[161]

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 UK.

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 US, TransUnion offers a special toll-free number for placing credit freezes, credit monitoring, and credit report, which is a step in the right direction.[162]

---

161 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.

162 See http://www.transunion.com/corporate/personal/consumerSupport/contactUs.page.

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.

Under the *Fair Credit Reporting Act* ("FCRA"), credit bureaus in the US must provide identity-related crime victims with a specific FTC-approved victims' statement of rights under credit reporting legislation.[163] 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 US 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.[164]

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 US 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.[165] 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.

---

163 15 USC. 1681g) ["FCRA"], s.609(d).

164 See: http://www.consumersunion.org/campaigns/learn_more/003484indiv.html.

165 FCRA, s.605B.

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.[166] Under US 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 US 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 US, consumers have a right to one free copy of their credit report annually.[167] 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.[168]

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."[169] 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.[170] 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

---

166 Under the FCRA, all US 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.

167 FCRA, s.612. See provincial credit reporting legislation in Canada, such as the Ontario *Consumer Reporting Act*, *op cit.*

168 FCRA, s.612.

169 FCRA, 15 USC. 1681s), s.621(f).

170 FCRA, s.605A.

identity fraud has already occurred, they can assist victims in mitigating damage in a number of ways.

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.[171]

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.[172]

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 US 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.[173]

---

171 FCRA, s.623(a).

172 FCRA s.605A; Ontario *Consumer Reporting Act.* S.12.3.

173 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 US *Fair Credit Billing Act*,[174] 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 UK limit consumer liability in the case of fraudulent transactions when the consumer has acted responsibly.[175]

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.[176]

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.[177]

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.

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

---

[174] 15 USC. 1693g.

[175] *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.

[176] FCRA, s.615.

[177] Ibid.

security breaches has become a major issue in the United States, where the reported incidence of breaches continues to rise.[178] 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 US states have passed security breach notification laws requiring that organizations notify individuals of breaches that expose their data to potential identity-related crime.[179] 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.[180] In Canada, Privacy Commissioners have published Guidelines for organizations responding to security breaches,[181] and the Australian Privacy Commissioner has issued a draft Voluntary Information Security Breach Notification Guide.[182] 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.[183]

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 US. 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.

Some employers provide identity theft/fraud insurance to their employees as part of their benefits package.[184] Alternatively, employers may cover the cost of an identity restoration service for employees who are victimized.

---

178 For a listing of data breaches, see <http://datalossdb.org/> (global) and http://www.privacyrights.org/ar/ChronDataBreaches.htm (United States).

179 See http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

180 OECD, *op cit*, pp.40-41.

181 See http://www.privcom.gc.ca/information/guide/index_e.asp.

182 See http://www.privacy.gov.au/publications/breach_0408.html.

183 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).

184 PrePaid Legal Services Inc. and Kroll are two companies that offer such products to employers. See http://www.prepaidlegal.com/ and htpp://www.kroll.com/services/fraud_solutions/.

Organizations whose security breach has exposed personal data to potential identity-related crime frequently offer credit monitoring services to affected individuals.