Standard Chartered

International Symposium on the
Prevention & Control of Financial Fraud
Prime Hotel, Beijing

19th - 22nd October 1998

PAYMENTS FRAUD

Presented by

Jeremy Platts
Area Head of Investigations
North East Asia

This paper, slides used and the comments of the presenter are those of the author and do not necessarily represent those of the Standard Chartered Group

Criminal activity tends to move in cycles as each new attempt to profit illegally is ruthlessly pursued until preventive action by the banking community raises the prospect of apprehension to the point where it is not economically viable for the criminal elements to continue. Fraud is just one form of illegal activity which constantly poses a threat to the banking industry as fresh innovative attempts are made to exploit the fund transfer system in a dynamic environment that is constantly changing as banks drive towards increasing revenues and market share.

This paper will attempt to address some of the perennial issues arising from a spate of frauds last year in Hong Kong affecting the Payments System which, although perhaps slightly different in each financial institution, provide some useful lessons from which we can all benefit.

The key components of the paper include a look at the symptoms of the fraud in the form of a case study which will then be followed by a diagnosis of the problem by assessing some of the fraud risk indicators. The paper concludes by offering some cost-effective recommendations to minimise future risks.

Payment fraud is nothing new. At first glance, the case study probably does not look too unusual or particularly complicated. Essentially, a number of telegraphic transfer application forms were submitted over a period of time to various retail branches in which a corporate customer was effectively requesting the bank to transfer a sum of money to an individual beneficiary who maintained an account at another institution. The signatures were duly verified, proper procedures and controls were followed, the transfer was effected and the beneficiary withdrew the proceeds in cash from his branch the following day, on Saturday

morning.
Everything appeared normal until the corporate customer, upon receipt of the remittance advice on Monday morning, advised the bank that it had not authorised any such payments.

The customer's signature on the transfer forms had been forged. The fraudulent applications submitted to the banks were each typed in exactly the same font and format. They were submitted over the counter in three different branches, were drawn on three different corporate accounts and favoured three different beneficiaries. They were each submitted late on a Friday afternoon (after the bank's cut-off time for processing local payments) and in each case the signature was very authentic.

The corporate victim accounts tended to belong to rather large customers for whom the amount of the transfer was comparatively modest, deliberately intended, it is believed, to avoid arousing suspicion if the account balance were to be checked. In the normal course of events at that time, there would not be any verbal contact between the bank and the corporate customer prior to effecting the transfer and they would be unaware of the transfer until they received the remittance advice through the mail.

In each case, the beneficiary of the transfer was an unskilled blue-collar worker with financial difficulties who had been paid the modest sum of HKD30,000- to be a willing scapegoat by using their identity card to establish the account and to approach the branch to withdraw the proceeds of crime which they then handed to a middle-man whose true identity they did not know. The aim of this ploy was to thwart the police investigation by distancing the fraud syndicate leaders from the scapegoat

who, on each occasion, was arrested and prosecuted by the police shortly after the commission of each offence.

The beneficiary account was either a recently opened account or a dormant account that had been reactivated for the purpose of the fraud. In one instance, an offshore account was used in the Portuguese enclave of Macau which is a 45-minute jet-foil ride from Hong Kong.

This is not a new type of fraud. It has been around the banking industry for some time. It tends more commonly to be committed by a collusive member of staff from the victim company who has a more detailed knowledge and understanding of the way the company operates. Alternatively, outsiders who are familiar with the bank's policy and procedures, could be responsible.

In these cases I would, however, suggest that there are a number of features which could serve as fraud risk indicators in future which alert staff would look out for. These are as follows:

- Does the corporate account have a history of making local payments by telegraphic transfer? If not, why would it suddenly start to do so now?
- Is it normal practice for a corporate customer to make payment locally by telegraphic transfer to an individual beneficiary?
- Regular corporate customers would generally not miss the cut-off time for local payments processing. However, on these occasions, the submission was delayed on purpose otherwise the corporate customer would have been advised the following day when banks open half day on Saturdays and this may have hampered the withdrawal of the proceeds by narrowing the window of

opportunity to the criminal.

- Large payments to individual otherwise inactive accounts just before a holiday are always worth double-checking.
- The forged applications forms themselves were a little unusual in so far as they provided additional information which would not usually be required in the normal course of business.

Clearly there is a need for some preventive medicine but there is a need to balance a series of counter-measures with the other important issues of customer expectations and service quality. Inevitably, the implementation of countermeasures will slightly affect service quality but customers can be assuaged on the basis that the precautions are in their best interests.

Such action will vary in each institution depending on the amount of risk they are prepared to accept but may include:

- Tighter internal controls on signature verification and approval process
- Standardised policy and procedures regarding payments implemented across all business divisions
- Centralised confirmation procedures with the customer.
- Special attention to
    - dormant accounts
    - hold-mail accounts
    - 3rd party beneficiaries
    - substantial reduction of account balance
- Regular staff awareness briefings
- Special arrangements with the customer

In conclusion, it is fair to say that fraud is just one of the risks involved in banking business and in the current economic downturn, it is reasonable to expect an increase in fraudulent activity. Ultimately, the best weapon to tackle the problem is a sharp and experienced workforce who have the awareness to look beyond the documents presented to them.