CONTROLLING FRAUD IN THE RETAIL SECTOR

Michael Shreeve
Head of Originator, Mondex Australia

Paper presented at the Fraud Prevention and Control Conference convened by the Australian Institute of Criminology in association with the Commonwealth Attorney-General’s Department and held in Surfers Paradise, 24-25 August 2000
Controlling Fraud in the Retail Sector

Overview

This paper addresses current and future activity involving cards. It covers current fraud and control techniques, the imminent shift in card technology from magnetic stripe to smartcards, and the implications of this for future fraud control and for the likely emergence of electronic cash. The presentation also outlines fraud control techniques for electronic cash in an environment where economic drivers may make it uneconomic to account centrally for each transaction.

Cards are a Key Area of Retail Payment and Fraud

Australian statistics suggest that in terms of value, cards are becoming a predominant means of retail payment (refer chart below).

The trend is similar globally. Data from the Nilson Report of May 2000 records that in 1999 there were:

- 1.2 billion cards (up 13% on the previous year)
- $US 1.9 trillion of purchases (up 16%)
- $US 0.8 trillion of cash advances (up 13%)

It is clear that there is great incentive for card fraud. If criminals can fraudulently access only a small proportion of these value flows, the rewards are enormous.
On-line Card Activity is Accelerating

On-line retail activity is already substantial and is forecast to increase dramatically. EMarteketeer in epaynews of 13 July 2000 records that:

- During 2000:
  - US on-line shoppers are expected to increase 73% to 63 million
  - Revenues will exceed US$37 billion

- By 2003:
  - Over 75% of US internet users will purchase on-line
  - Business to Consumer (B2C) revenues will exceed $US100 billion

As with retail activity generally, there is great incentive for on-line fraud. Criminals are finding it easier to exploit on-line activity, and on-line fraud is estimated to be considerable:

- GartnerGroup estimates that on-line retailers are 12 times more likely to be defrauded
- In 1999 Visa is reported to have lost $US1.3 billion from e-fraud (Australian Financial Review, 10 August 2000)

Australian on-line retail activity is also forecast to grow dramatically. The chart below forecasts that by 2002, annual on-line sales are expected to approach monthly retail sales.

Australian on-line sales also forecast to grow dramatically

Types of Fraudulent card use

Merchants obtain details of genuine cards in a number of ways, including:

- Taking multiple paper vouchers
- Skimming. This involves recording card details electronically without the card owner’s awareness, usually by swiping a card’s magnetic stripe through a small piece of equipment.
Fraudsters acting as consumers act as if they have genuine cards in a number of ways, including using:

- Replicated cards from skimmed data
- Stolen cards
- Newly generated cards that have the characteristics of genuine cards – algorithms are available on internet sites that describe the numbering characteristics of genuine cards.

Fraudulent card use takes place across all retail channels, including face-to-face purchases on the high street, phone banking, and the internet.

The extent of skimming is considered to be substantial, but accurate data is hard to obtain. A report in Time Magazine of 12 June 2000 indicated that skimmers in the US reaped about $US125 million. A report in the Sydney Morning Herald of 13 November 1999 indicated that skimming costs in Australia could be as high as $A500 million per year. It would be extraordinary if the value of skimming in Australia was higher than in the US. Both estimates are probably wrong, but the key point is that skimming is a real issue and one that involves hundreds of millions of dollars globally.

**Fraud control measures for cards**

This section discusses three fraud control measures:

- Tighter procedures
- More secure communications for on-line transactions
- Move from magnetic stripe to chip-based cards

**Tighter procedures**

For consumers, the sensible approach is to keep the card in sight at all times, to prevent skimming. However, this does not completely accord with current cardholder and merchant behaviour. The typical behaviour in restaurants, for example, is to provide the card to a waiter, who removes it from the table in order to create the record for signing. While the card is out of sight it may easily be skimmed. While tightening the procedure is simple in theory, it is unlikely to take place in practice.

For merchants, there are a number of areas in which it would be prudent to tighten procedures.

- Signature checking is an obvious one to mitigate against use of stolen cards. However, in practice, signature checking often does not occur, and when it does occur it is often cursory. It is possible that a merchant might feel that a signature check suggests that the merchant doubts the integrity of the customer, and that this insult might reduce the prospect of future patronage. Signature checking may assist to identify stolen cards, but cannot assist with fraudulently-created cards.
- Remote verification of the card to check its limit, or whether it is stolen, is also a sensible and obvious procedure that does not appear to be used all the time. The procedure takes time (which involves cost) and again risks insulting the customer.
Useful confirmation techniques used by some merchants for unsigned phone orders include:
- A call-back policy
- Verification that billing and delivery addresses are the same

It would also be helpful if merchants put firewalls around their databases containing the card details of customers, so that this information could not easily be accessed by criminals.

**Secure Communications for on-line payments**

For rapidly-growing on-line payments, where the rate of fraud appears to be considerably greater, more secure communications are an obvious area of interest. Three options are outlined below.

- The most-commonly used form of security is the Secure Sockets Layer (SSL). This essentially establishes an encrypted line between the consumer and merchant, designed to prevent a third party accessing the messages. This is used reasonably often, but the cardholder details remain available to the merchant in unencrypted form, and therefore can still be used for skimming.

- Microsoft has a proposal called Microsoft Passport in which Microsoft would securely store details of consumers and merchants and act as a secure hub for routing and verifying transactions. Many entities have aspirations to act as a central hub to verify the credentials of parties to a transaction. These range from financial institutions, to telcos, to regulatory agencies. It will take considerable time to see the outcome of concepts like this.

- Secure Electronic Transfer (SET) is a technique promoted by card companies Mastercard and Visa. The concept is that financial institutions will issue digital certificates to authorise consumers to merchants, and merchants to consumers. A merchant will not know the details of the consumer’s card, but will have an effective guarantee from the consumer’s card issuer that the payment is genuine and authorised. Similarly, the consumer will know that the payment is to a genuine merchant authorised by a financial institution. The execution of this concept is considered complex by merchants and at this stage is not much used.

Work is clearly progressing in the area of secure communications, and this will be affected by developments in secure identification generally. The goal is to get the right balance of convenience, cost and security. At this stage it remains unclear as to which standards that will emerge as being ubiquitous.

**Smart Cards**

Smart cards involve replacing (or supplementing) the magnetic stripe on a card with a computer chip embedded in the card. The chip is similar to the chip that resides within a personal computer or a mobile phone. It contains data (like a magnetic stripe – but with much more capacity) and a micro-processor that can undertake computations (which a magnetic stripe cannot do - hence the term “smart” card). Latest generation smartcards are as powerful as early personal computers.
In a fraud context, the advantages of smartcards over magnetic stripe include:

- Physical tamper resistance—they cannot be skinned
- Logical security including potential to apply strong cryptography to data transfer – security is increased by the greater data capacity of the chip, and the ability to undertake cryptographic computations within the tamper-resistant chip itself, rather than in an interface device.

**Development of Smartcards**

In a business context, smart cards are becoming more popular because they have much greater functionality than magnetic stripe cards. Modern smartcards can have many applications within the one chip; such cards are called multi-application smartcards. Multi-application smartcards require an operating system. Several systems are aspiring to become an (or the) industry standard. These include:

- MULTOS
- Java Card
- Microsoft Smartcard for Windows

The merits of the different operating systems are not discussed in this paper. However, in terms of fraud prevention, MULTOS has the best credentials, having been assessed by Europe’s Information Technology Security Evaluation Criteria (ITSEC) as having a security rating of E6 High. This is the highest rating possible to be attained and no other commercial product has yet attained this level of certification (except Mondex, an electronic cash application associated with MULTOS and which operates on the MULTOS operating system).

Smartcards have been around for many years. Smartcard promoters have fairly consistently forecast wider and faster usage than has in fact occurred. Nevertheless, it is starting to appear that the age of the multi-application smart card is finally arriving.

The UK is in the process of moving its bank-issued cards from magnetic stripe to chip, and it is expected that 40% will be converted during 2000 and that the process will be completed by the end of 2002. Visa is forecasting that the transfer to chip will be completed by 2006 in Asia Pacific and by 2010 worldwide. A key driver of the move to chip is to avoid the fraud associated with magnetic stripe.

Another example comes from MYCAL, Japan’s fourth largest retailer. The Asian Banker Journal of June/July 2000 noted that MYCAL had already issued 1 million chip-based cards from a card base totalling 6 million. Fraud prevention was the main motivation – MYCAL’s Chairman stated that fraud rates doubled last year and YEN200 billion was fraudulently used. Other reasons for the move to chip were the ability to load other applications onto the cards, including loyalty programs and an electronic purse.

The ability to load multiple applications onto a chip is a key business driver for smartcards that has only been available over the last year or so. Some key business opportunities include:

- Credit/debit applications to prevent fraud
- Mass transit for efficiency, including contactless cards
Remote secure identification, using cryptographic features supported by smartcards

Loyalty applications

Electronic cash

The ability to operate multiple applications on the one chip card make the cost of the card and related infrastructure much more attractive, and improve the business case for each individual application.

Electronic cash (e-cash)

As multi-application smartcards become more widespread, the business case for e-cash becomes more attractive. There are a number of areas in which e-cash is proving or expected to be successful:

- Internet micro-payments, where it is not cost effective to process a traditional payment
- Campus (such as an educational, military or corporate facility) where it is relatively inexpensive to provide for intensive local use of e-cash
- Lotteries, for efficiency of payment and control of fraud
- Unattended Point of Sale, such as vending machines and parking meters, because having the right change is never a problem with e-cash
- Cash replacement in the third world, where delivery and storage of electronic cash can be much more secure than traditional cash
- Interactive TV, where e-cash is immediate, secure and cost-effective

Fraud Control & Risk Management for (Mondex) e-cash

The objective is to ensure that an e-cash scheme remains economically viable, even under attack.

The task in putting together a risk control strategy is to:

- Understand the environment
- Prepare appropriately
- Monitor compliance of scheme members
- Detect and quantify and counterfeit value in the system
- Incident response – to stop/constrain the flow of any fraudulent value

There are two broad types of smartcard-based e-cash schemes:

- Those that seek to centrally account for each transaction – this is the intent of the specifications promoted for a scheme termed CEPS (for the Common Electronic Purse Standards)
- Those that seek to centrally account for high-value transactions, but allow some low-value transactions to be recorded locally, on the chip itself (such as Mondex)
Studies indicate that for large scale e-cash implementations, Mondex–type schemes will be much less expensive. This is simply because Mondex avoids the cost of centrally accounting for each transaction. Indeed, if e-cash transactions are to be centrally accounted, they become less like cash and more like centrally accounted debit and/or credit cards.

Reliance only on the fact that a scheme intends to centrally account for each transaction, can give a false sense of comfort about the ability to undertake fraud control and risk management. The problems that arise can be illustrated by following through an example of what might be associated with a centrally-accounted e-cash system:

**Loading e-cash**

The cardholder loads e-cash onto its card in return for giving payment to the provider of the e-cash load facility. The provider will need to send the details to the cardholder’s issuing institution, who will:

- depending on the type of payment offered for the e-cash, debit the cardholder’s account (perhaps a savings or credit card account)
- credit an e-cash float account (to cover the e-cash liability that has been created)
- arrange to post the details to the centralised shadow e-card accounts (for purposes of monitoring and risk management)

There is likely to be a lag between the loading of the e-cash, and the posting to the centralised account, unless the parties are prepared to pay for expensive real-time systems.

**Spending e-cash**

The cardholder next spends e-cash with some retailers. The next steps will then be:

- The retailers redeem the e-cash with their acquiring banks
- The acquiring banks then arrange to:
  - make a claim on the e-cash float
  - adjust the centralised shadow e-card accounts

**Fraud control and risk management**

At this point the risk manager, looking at the centralised e-card accounts will encounter challenges:

- Timing lags will occur between the time of the transactions in e-cash, and the time at which the details are posted to the centralised accounts
- Sequence issues will arise, because it is likely that transactions will arrive at the central site occur out of chronological order e.g. expenditure details could arrive before load details
- Systems problems will inevitably mean that some data will be delayed
- False positives may occur for fraud, because it will appear that some cardholders have spent more e-cash than was legitimately loaded onto their card – the truth will be that the details of the legitimate load simply have not yet been forwarded and processed at the central site.
Thus indications of fraud could simply be false positives caused by transaction details arriving out of sequence. The desire to maintain good customer relations will tend to make risk managers cautious about responding quickly to possible indications of fraud.

A second issue relates to truncation of data. Once e-cash schemes become ubiquitous (which will be some time away) there are likely to be several e-cash transactions per person per day. This amounts to billions of transactions per day globally, and at least tens of millions of daily transactions in Australia. Large transaction volumes inevitably lead to economic pressure to truncate the data at source and provide it periodically in batches (and possibly in summary form). This would mean that the risk manager has only partial information to rely on.

The likely scenario for a widespread scheme is thus one of huge volumes of low value transactions, where data cannot be economically processed in real time. Any central site is likely to experience problems of timing and sequencing, and data will probably be truncated. This type of scenario is one that locally accounted schemes such as Mondex are well equipped to handle, because the risk management design has been based on just such an environment and built in at all levels of the scheme.

Mondex risk management can be considered at three levels:

- Prevention
- Detection
- Recovery

**Prevention**

The Mondex prevention strategy is designed to prevent any business case for Mondex fraud emerging. The quality of the controls is extremely high, as evidenced by the ITSEC E6 High rating. The overall approach is very comprehensive and sophisticated, and is not covered in detail in this paper. However, some key features include:

- Highest levels of physical security, including
  - data destruction if the chip is physically breached
  - the purse can be locked by a PIN, so that a stolen purse cannot be used
- Logical cryptographic techniques to ensure the integrity of the value transfer including:
  - RSA crypto
  - Crypto set within the tamper-resistant chip (rather than in more easily-accessible interface devices)
- On-chip controls within the chip itself, including:
  - Limits on the amount of value that a purse can hold
  - Limits on the amount of value that can flow through a chip before it becomes locked and needs re-activating by the issuing institution
  - Constraints on the particular types of purses that each individual purse can pay to (for example, a high value bank purse could pay to a lower value bank purse, but not to a consumer or merchant purse). The ability to structure the direction of value flows between the various types of purses allows for more-predictable behaviour and tighter risk management.
Detection

Mondex is designed to make the business case for fraud so unappealing that it should not occur. However, if fraudulent value were to be created, then it should be identified quickly. Mondex value in each currency is created in a highly secure environment and provided only to that currency’s Originator. The Originator will provide the value only to eligible scheme members – these transactions are centrally accounted. The scheme members will provide value to clients (typically consumers) – these transactions are also centrally accounted (by the issuer). Consumers will spend the value with merchants and the merchants will redeem the value with their sponsoring member - the redemptions by merchants are also centrally accounted (by the merchant sponsor). Thus the only transactions that are not centrally accounted are transactions between two consumers, and transactions between consumers and merchants – while these transactions are not accounted for centrally, they are accounted for on the card itself (for the last ten transactions).

The Originator and members will monitor closely the usual flows with each member, merchant and consumer – data is monitored at least daily. If fraudulent value were to be introduced, the flows would alter. In particular, redemptions of value would start to be large in relation to issues of value, reflecting the illegal issuance of value from another source. Highly-sophisticated statistical and mathematical techniques are used to monitor the various value flows and identify any unusual activity.

Recovery –Incident Response and countermeasures

A range of countermeasures are available, depending on the severity of any attack.

Some are built into the chip itself eg if an unusually large volume of value flows through a chip the chip will become locked and need to be returned to the issuing institution for inspection and resetting. Issuers also have the capacity to retain a suspect card when it comes into contact with the issuer.

A particular feature of Mondex is the ability to migrate from one cryptography scheme to another. This is achieved by issuing cards with more than one crypto scheme. At an appropriate time, Mondex Originators will issue instructions that will cause each interacting card to migrate irrevocably to the new crypto scheme, and to similarly migrate each card they interact with, so that the migration instruction cascades quickly throughout the entire active card population. Typically, member cards would migrate first, then merchant cards when they redeem to the member, then consumer cards when they interact with a migrated member or a migrated merchant or a migrated consumer. In a few days the entire active card population would have migrated to the new crypto scheme. This has the benefit of removing old cards (without the new crypto scheme) from the active card population – in this way the Mondex scheme can always be assured of having active only recent cards; recent cards will be more secure than earlier cards because of ongoing technology improvements.

Another potential benefit of migration arises in the unlikely event of fraudulent value being created. Such fraudulent value would need to use the existing crypto scheme - once active cards have migrated to the new crypto scheme, there is no value in the ability to create fraudulent value using the old crypto scheme, since no converted card will be able to accept it.