# Mouse clicks and dirty tricks

In the June 2000 edition of *Platypus Magazine* (p.2) Commissioner Mick Keelty referred to an article that appeared in the *Business Review Weekly* on April 11 this year. *Mouse Clicks and Dirty Tricks*, by Patrice Gibbons raised the question about private enterprise needing to accept responsibility for reducing the criminal use of technology that the corporate world introduces.

Due to a number or enquiries about this article, the author and the Business Review Weekly have granted permission for the article to be reproduced here in full.

*Online credit-card fraud is rife in Australia and is costing retailers hundreds of millions of dollars a year, But although merchants are losing money, the banks that provide them with online payment services are making hundreds of thousands of dollars through transaction fees and interest on fraudulent purchases.*

Banks will not take responsibility for online credit-card transactions because merchants do not see a signature being made. Tony Gattari, managing director of the online developer and retailer Smartbuy, says online merchants must cover losses from fraudulent transactions themselves, even though the banks cover the losses of merchants in the physical world. "Online merchants are faced with the full liability because banks are not willing to take the risk," he says.

Although they escape liability on fraudulently purchased goods, banks still receive a transaction fee from the purchase. The fee is a percentage of the transaction value and can range from 1 per cent to as high as 4 per cent, depending on the merchant's agreement with the bank. Interest also is accumulated from the time the purchase is made until the cardholder lodges a complaint and the bank confirms that the transaction is fraudulent, a process that can take several months.

Research conducted last year by Gartner shows that credit-card fraud in the United States is 12-18 times higher online than in offline transactions. Richard Harris, the vice-president for e-business intelligence at Gartner Asia-Pacific, believes the figure is similar here, although his company has not researched it locally.

Credit-card fraud is easier online because no signature is required. The card number and expiry date are the only essential details, and they can be easily obtained by swiping a card through an electronic machine that records the number, expiry date and name from the magnetic strip. National Australia Bank (NAB) says its merchant customers lost about $700,000 in the three months to December 31 last year through online credit-card fraud, and the online gambling company My Casino lost $4.3 million between March and July last year through the fraudulent use of credit cards. (My Casino lost the money through a well-organised group of gamblers using more than 1000 fake or stolen credit-card details.)

Critics of the banks' approach to online fraud, including Gattari and Rafael Chavan de Montero, the chief executive of the online book retailer OzBooks, says there is no incentive for banks to change the arrangement. "Where is the motivation for banks to try to improve the situation?" Gattari says. "There is no reason for them to move because they are not suffering."

Stephen Carroll, a director of the Australian Bankers Association, says transaction fees cover the cost of providing payment services to merchants. "Whether it is fraudulent or not, the cost has to be recovered," he says. Carroll says online trading has advantages for merchants and the onus is on them to verify the cardholder's details when goods are delivered. This, he says, would save companies money because fraudulent purchases would not be handed over. However, they would still be hit with a transaction fee.

One of the reasons online retailers are struggling to have their case heard by the banks is that they do not have an industry-wide lobbying group. Gattari says the industry needs to form an association to give online retailers lobbying power with the banks and government. "There is strength in many and weakness in few," he says. Chavan de Montero says the issue needs to be discussed in Parliament.

Retailers want a new system between merchants and banks to match the credit-card number with the owner's correct name and address before processing. Banks hold this information, but they are reluctant to reveal it, claiming that it would breach privacy regulations. But Chavan de Montero says there would be no breach of privacy if the banks confirmed the cardholder's details with a yes-or-no answer, rather than giving out the details to merchants. He says banks also fear that a pooling system would give other banks access to their customers, thus encouraging poaching.

Fraud would be cut by introducing a system that allowed merchants to cross-check details with all banks. One customer making a purchase from the OzBooks site listed his name and address as Mickey Mouse in Disneyland. His transaction was approved because the credit-card number was valid. But because the details were ludicrous, Chavan de Montero called the bank. The bank refused to confirm the details because of privacy restrictions. OzBooks cancelled the order. Several weeks later, Chavan de Montero met a journalist who mentioned he had been testing the site with a made-up credit-card number and using the name Mickey Mouse.

Banks reject claims that they are unwilling to assist merchants, pointing to their recent efforts to help detect fraud. In June last year, NAB introduced software that compares each transaction against the merchant's normal transactional profile. The software detects multiple transactions on one card: a high number of transactions might indicate an organised fraud ring.

Nick Kennett, general manager of cards and financing products at Commonwealth Bank, says the bank monitors any changes in normal spending patterns for each credit card. A transaction was stopped recently after a purchase was attempted in a store in Bangkok with a card that had been issued in Sydney just three hours earlier.

But Chavan de Montero says the software used by the banks largely protects consumers, not retailers. If a fraudulent transaction is detected after it is approved, the merchant still faces a transaction fee.

Gattari admits that merchants must take some responsibility for fraudulent purchases, and many have taken steps to detect fraudulent transactions before they are approved. They have introduced systems to identify cards from geographical areas where credit-card fraud is high, and to alert them to large amounts being spent on a card in one day. Many are also contacting customers when a transaction looks suspicious.

Smartbuy set up an e-commerce site for the retailer Tandy Electronics in February (Woolworths acquired Tandy in April this year). Gattari says 30 per cent of the initial purchases attempted were fraudulent. Smartbuy has a staff member assigned to checking each transaction on the Tandy site. If an order looks suspicious and the customer cannot be contacted through the details he or she provides, the transaction is cancelled.

Several fraudulent transactions have slipped through the OzBooks site. They include those by a man in Germany buying books using the credit-card details of a man in Peru. And when OzBooks sent an order to Yugoslavia, several months later the transaction was reversed and it was discovered that the real card owner lived in Peru.

Gattari says many people do not consider online fraud to be as serious as stealing from a store because they cannot be traced and there is little risk involved. One customer trying to buy from the Tandy site had the right credit-card number, but the wrong expiry date. He tried to make a purchase 42 times using a different expiry date each time. When this approach failed, he called Tandy and said there was a problem with its Web site. "People don't seem to see that this is stealing," Gattari says.

One solution would be to attach personal identification numbers to credit cards. As with an EFTPOS card, the personal details would be useless unless the user also knew the number.

Smart-cards have also been promoted as a way of reducing online fraud: they contain personal information about the owner that can be cross-referenced with the card number. But Gartner's Harris says there is not enough incentive for consumers to stop using credit cards. Most are attached to reward programs, which give consumers another reason for using them. Gartner says about 93 per cent of online purchases in the three months to September 30 last year were made on credit cards.

"I can't see this changing in the next two to three years," Harris says. "The fundamental thing merchants have to do is introduced fraud-reduction strategies."

## CREDIT CRIMES

**Banks will not take responsibility for fraudulent online transactions because merchants do not see a signature.**

**Merchants still face a transaction fee on fraudulent transactions, of between 1 per cent and 4 per cent of the value of the purchase.**

**National Australia Bank merchant customers lost about $700,000 in the three months to December 31, 2000, through online credit-card fraud.**

**Just on 93 per cent of online purchases in the three months to September 30 last year were made on credit cards; the other 7 per cent were conducted using methods such as direct debit.**