Bonus Section B

ELECTRONIC PAYMENTS INTERNATIONAL

Issue 102, November 1995

INSIDE . . .

Chase Bank joins IBOS

CHASE MANHATTAN Bank, one of the largest US corporate banks, has signed as an investment partner to the Interbank On-line System (IBOS).

The New York-based institution took a 24.05 percent stake in the Royal Bank of Scotland/Banco Santander-led real time global payments and electronic commerce system on November 6.

The addition of one of the world's largest corporate cash management institutions has given a significant boost to IBOS which, despite signing several institutions since its creation, has failed to live up to its early promise.

Transaction volume was believed to be low. However, Sean Verity, chief executive of IBOS, told *EPI* transaction volume is growing in "3-digits".

Verity said the addition of Chase is significant both in terms of the size of its investment and the profile it adds to IBOS. "We are trying to build working relationships with global players in corporate cash management institutions," he said.

"We were looking for someone like this to share our vision of the future. It is a big vote of confidence in the system," Verity said.

While Chase will undoubtedly renew interest in IBOS, Verity said the organisation is not looking to sign more partners straight away. "We don't want to take on more than we can deliver. We are trying to focus on our real areas of opportunity."

Responding to the disappointing performance of IBOS in the past, Verity said this was due to bad positioning, particularly in relation to SWIFT, the global message carrier. "What happened was the articulation of our strategy was counter-productive. We are not in competition with SWIFT, although this was implied. We will have a rapprochement with SWIFT."

He said IBOS is a "marketing-driven" company, with no aspirations to compete

Continued on page 11

Eurotransfer expands

BANQUE BRUXELLES Lambert (BBL), Belgium's second-largest commercial bank, has expanded its cross-border payments system, Eurotransfer, to include the Netherlands, the UK and France, which, with Germany, represent 80 percent of all Belgian transfers within Europe.

Following the freezing of the activities in September of B.epsys, the Belgian European payment system owned by seven banks, BBL hopes Eurotransfer will be extended to the rest of the EU countries within the next six months.

Eurotransfer was launched in April 1994, on a B.epsys and GZS technical platform, to enable BBL customers make low-value deutschmark payments to Germany. It proved successful with about 3,000 credit transfers a month, so the service has now been extended.

According to Paul Massea, BBL's product manager for international transfers, the bank has signed non-exclusive bilateral agreements with its traditional correspondent banks in four countries, but declined to name them.

Payments will be limited to Ecu2,500 ($3,250) while a fixed charge of BFr310, plus VAT will be levied. It will take six banking days to make the payment using SWIFT's IFT platform.

As of November 15, the Eurotransfer service is available in all BBL's 1,000 branches and 150 banking units throughout Belgium.

Carol Power

30 years on, fraud continues to grow

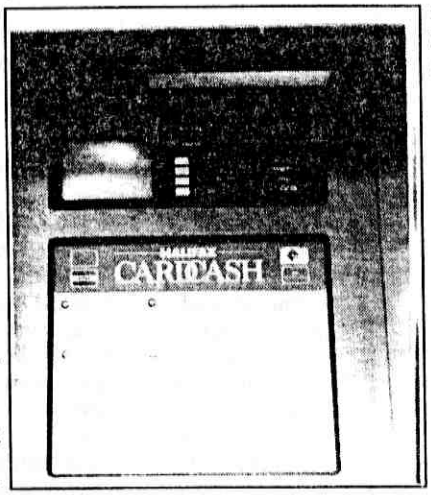
The most common types of fraud losses are typically very low- tech, but possible to reduce if financial institutions can better educate their cardholders. *Dr Barry Schreiber analyses the most common crimes**

After 30 years in business, the ATM is increasingly being recognised as a convenient vehicle for fraud. At night, the ATM provides a much more attractive and anonymous location for attempting fraud than in the bank lobby during day-time hours, under the gaze of bank employees, possibly security officers and certainly video cameras.

A 1987 Bank Administration Institute national survey of large US financial institutions found 63 percent of reported ATM fraud was due to "unauthorised card use", typically lost or stolen cards, and unauthorised family or friends use of cards.

The second largest category, about 33 percent of the incidents, was "fraudulent ATM customer activity", including empty envelope deposits and other worthless deposits.

These most common types of fraud losses are typically very low- tech, and in fact, are possible to reduce if financial institutions can better educate cardholders about card and personal identification number (PIN) security; and are able to implement tougher policies on the immediate crediting of ATM deposits. The constant testing of ATM security integrity by would-be fraudsters was illustrated recently in the state of Oregon.



A bogus cash dispenser installed in a shop in East London which was used to record information from Cashpoint cards which were then used to withdraw £120,000 from customers' accounts. Graham Moore and Anthony Hodges were found guilty at Southwark Crown Court in September.

Case study No 1 — Oregon TelCo $346,770 loss on one stolen ATM card

On Friday night, November 18 1994, the ATM card and PIN of Oregon TelCo Credit Union member Karen Smith were stolen from her purse in her locked vehicle in a suburban Portland, Oregon high school parking lot. The thieves quickly used the stolen card and PIN for an unauthorised cash withdrawal.

Because newly-installed Credit Union ATM software failed to check for a 24-hour withdrawal limit, the card thieves used the one stolen card 723 times over the following 54 hours at 48 Oregon ATMs. The card thieves withdrew a total of $346,770. When Karen Smith's account was nearly empty, the thieves simply made empty envelope deposits to gain immediate deposit credit in the account. A total of five empty envelope deposits were made, totalling $820,500. Four of the 48 ATMs had hidden cameras which took pictures of the thieves. Four people were arrested for these crimes, which illustrated two costly ATM system problems and the constant testing by criminals of the ATM system for fraud resistance.

Counterfeiting ATM cards

Much more troublesome for ATM fraud security is the spread of information indicating how easily a legitimate magnetic-stripe ATM card can be counterfeited.

Among the early detailed explanations of how to fabricate a counterfeit mag stripe card was the April 25 1993 London *Sunday Telegraph* feature, which ran a three-photo layout across one page showing:

a) a thief "shouldering" the PIN number of an unsuspecting ATM user and retrieving the discarded ATM transaction receipt upon which the full bank account number was printed; b) the thief using a desktop computer to encode the stolen card number and PIN on a blank mag stripe card, and c) the thief using the counterfeit ATM card to withdraw £10 from an ATM. Explanations and demonstrations of mag stripe card manufacturing have appeared in several print and broadcast media reports since then.

Case study No 2 — Bogus ATM in Connecticut used to collect ATM account numbers and PIN for $107,460

The first publicised large-scale theft of ATM card and PIN numbers occurred at a "bogus" Fujitsu ATM installed by fraudsters for 12 days in a shopping mall outside of Hartford, Connecticut.

Using the legitimate ATM account numbers and PINs supplied by unsuspecting users of the "bogus" ATM, scores of counterfeit cards were manufactured. More than $107,000 was stolen by the fraudsters using counterfeit cards before the US Secret Service arrested three men in the scheme.

Case study No 3 — Home-built fake ATM used in London for £120,000 fraud

On September 14 1995, two men were convicted in London of installing a well-built home-made copy of an ATM through the wall of a small shop in east London, which ostensibly brokered Hambro UK mortgages.

The realistic machine captured account and PIN numbers, enabling the London fraudsters to fabricate more than 100 counterfeit mag stripe ATM cards which were used to withdraw more than £120,000 ($186,000) from genuine ATMs around England. To illustrate the speedy international spread of ATM fraud vulnerabilities, the following example is offered.

Case study No 4 — the "Lebanese Loop"

A group of fraudsters believed originally to be from Lebanon have developed an ATM card trap which uses a strip of 35mm film to capture an unsuspecting ATM user's card in the ATM card-reader.

After the legitimate card is trapped, a "helpful stranger" appears and states that he, too, lost his card in the same machine, but got it back by re-entering the PIN number. The fraudster leaves having spied the correct PIN number and returns after the victim leaves the ATM to retrieve the trapped ATM card.

The "Lebanese Loop" fraud is often perpetrated on a Friday, which means the card can be used for at least the weekend until the banks re-open on Monday and can receive the customer's complaint about the lost card.

The "Lebanese Loop" is believed by the International Association of Credit Card investigators first to have been employed in Venezuela for at least $500,000 in losses and then quickly to have been exported to Spain, Argentina, Canada and the US.

The future of ATM fraud

ATM fraud schemes certainly will become more numerous, and more sophisticated in the near future. Line security compromises, theft of ATM account and PIN numbers, line spoofing and attacks by computer hackers are all expected. Any successful ATM fraud may be exported internationally.

Barry Schreiber

ATM Fraud Solutions:

Meanwhile, what can financial institutions do to minimise their fraud loss risks? Consider the three C's:

1) **Cameras** should be considered at all ATM locations. While not being able to prevent ATM fraud, camera images of fraud perpetrators have been enormously useful to law enforcement investigations of major ATM fraud cases, including the Oregon TelCo fraud and the bogus ATM fraud in Connecticut.

2) **Controls** on ATM cards must be established. A written financial institution ATM Fraud Policy should be considered, specifying practices to be followed for: card issuance and replacement, PIN assignment, maximum number of PIN attempts, use of transaction cameras with date, time and transaction number stamped on each image, amount of cash back allowed on ATM deposits, how soon to credit ATM deposits, customer signing affidavits for unauthorised ATM transaction claims and minimal conditions for, and evidence needed to prosecute an ATM fraud.

3)**Co-operation between financial institutions and law enforcement agencies**. Both local and international ATM fraudsters have no "brand name" allegiance. They will steal money from everyone they can. City-wide and regional financial institution fraud clearing houses share information about ATM enforcement.

In Atlanta, an extremely well-organised Nigerian/West African Fraud Task Force is co-ordinated by US Secret Service Agent Tom Johnston at telephone 1-414-331-6111. The force publishes a monthly newsletter and has made significant progress on frauds committed by this group.

In the very near future, a secure, authorised-access, electronic bulletin board will be needed for international law enforcement investigations and financial institutions sharing ATM and other fraud information. Who will be the leader to establish real-time international information sharing to combat ATM fraud?

The first 30 years of ATM use have been astoundingly successful worldwide. With appropriate planning and communication between fraud enforcers, the future can remain equally bright for the expanded use and functions of ATMs. ♦

**Barry Schreiber is a professor of criminal justice at St Cloud University in Minnesota. He has developed expertise in ATM crime and security in the past ten years: including US national surveys of ATM crime and fraud; membership on national task forces; and by writing the book "ATM Security in the 1990s". He is editor of the monthly "ATM Crime and Security Newsletter".*