



Latin American Credit

Latin America follows U.S. strategy in fighting fraud

February 01, 2010

By: Wayne Tompkins

Executives of one Mexican bank tell of forklifts commandeered by thieves to rip ATM machines out of walls, after which they are hacked and mined for customer data. In Brazil, a bank that outsourced its ATM maintenance found that the contractor had placed data stripping devices in the machine to copy PIN numbers from customer cards. A Colombian retailer was done in by his own employees, recounting how they had collaborated with a crime ring to place devices at the register to copy credit card data for use in cloning cards.

While advances in IT security have made such schemes harder to pull off in the United States and Europe, they remain pervasive in Latin America and other regions of the developing world, said John Price, managing director of market intelligence services at Miami-based Kroll-InfoAmericas, which led a credit fraud workshop at recent Latin American credit card industry conference.



"In the United States and Europe, where security measures are pretty solid, the only channel remaining open to fraudsters is a very high-tech channel," Price said.

In a research report for Kroll, Price noted that most fraud in Latin America is still committed through low-tech schemes. For example, some fraudsters will break into ATM machines and install a card reader to "skim" the card's information. From there, the credit card number is sold on the secondary market where it winds up in the hands of counterfeiters.

Skimming technology has become sufficiently inexpensive, portable and user-friendly to allow everyone from waiters, store clerks and airline ticket agents to be parties to the crime. Failing that, corrupt and poorly screened employees and vendors can steal vital information.

"The credit card fraud numbers are much more prevalent in Latin America, as well as other developing countries, primarily because they don't have the means to properly screen their own people or evaluate the IT loopholes in their own security systems," Price said.

George Harper, a partner in the Miami law firm Harper Meyer, said he sees the fraud trend in the region as "almost a logical occurrence."

Not only does Latin America tend to follow U.S. trends, countries such as Brazil, Colombia, Argentina and Mexico have seen their electronic commerce explode over the past few years.

"That means there's going to be fraud the same way there was here, the same experience," Harper said. "It is unsophisticated theft with dishonest employees and the lack of due diligence. With the forklift, I wonder if anyone happened to notice?"

Harper said the U.S. dealt with these types of low-tech crimes several years ago before its securities procedures caught up with the thieves.

Now Latin America is fighting the same battle.

"We found ways to combat it; they will too," Harper said.

As more Latin American consumers become banked and get access to credit cards and other financial instruments, businesses and governments in Latin America will need to act against credit card fraud before it gets any worse. The good news is that affordable, low-tech solutions can go a long way toward addressing the problem.

Price said "huge dents" could be made in the level of fraud exposure through preventative measures.

While the practice of credit card fraud itself is not likely to discourage investment in the region, Price said it raises the cost of doing business and customers are ultimately the ones who absorb those costs in the form of higher fees and interest.

"You're raising the cost of credit which, in turn, limits its accessibility," Price said. "Certain retail businesses might not consider entry into a market until they feel comfortable with the level of accessibility to credit. Instruments can not realistically be introduced to the financial services industry in a given market until there is significant access to credit."

EMERGING MARKETS

According to Price, card fraud globally took in an estimated \$5.5 billion in 2007. While he calls that a startling number on the surface, it is just 0.05 percent of the total card transaction volume, 2 percent of what card companies charge for their services, "and even less than what issuers earn in interest from customers."

But the numbers are much higher in emerging markets. In Brazil in 2008, according to Kroll's analysis, credit card fraud reached about \$300 million, or 0.15 percent of the transaction volume — three times the global average. This in spite of the fact that Brazil has what's generally regarded as Latin America's most sophisticated banking system. In Colombia, losses approach 0.25 percent of total card volume, or eight times the United States average.

SECURITY TRAILS GROWTH

Jorge Gutierrez, an attorney with Tew Cardenas in Miami who put together Brazil's first private label credit card deal in Brazil several years ago, said growth is likely to continue to outpace support structures such as security systems.

"We discovered really early on that the penetration opportunities there were really huge because only 3 percent of all people with the ability to have bank accounts actually had bank accounts," Gutierrez said. "So the credit card phenomena has huge growth potential. The reality is they have not been able to keep up with the hackers because they are just starting from Level 1."

In one case, a Caribbean bank's own IT employees had downloaded cardholder identities from the bank's computers.

The incidence of credit card fraud is more pervasive in some Latin American countries than in others.

"It's a country-by-country thing," said **Dennis Nason**, a Miami international banking consultant. "You don't get this in Chile, where it's much more sophisticated, or in Panama. It's the level of the sophistication of the market that makes the difference. You've got 20 countries down there, so you have to peel the orange a little bit."

Harper said that while the issue of identity theft insurance has not yet become significant in Latin America, it will.

"Right now, if something like that happens there is not an awful lot that you can do about it," he said. "You can complain to the bank, and the bank will take measures in the future."

But in the meantime, the customer is in limbo.

"The courts are inefficient and extremely busy and your request for justice is probably not going to be heeded too well," Harper said.

Where consumer protection laws exist on the books of many Latin American countries, the resources and political will to enforce them remains lacking — adding to the favorable climate for fraud schemes.

In his research and conversations with Latin American bankers, Price learned that while employees and vendors are responsible for much of the fraud, "all the guilty parties had some criminal record that had not been discovered in the internal background checking process of hiring or contracting."

In the case of the smash-and-grab forklift theft, the surveillance equipment and systems were not functioning, victims of budget cuts.

The most galling conclusion, he said, was "how preventable" most of these episodes were.

"In the U.S. we just assume the system will protect us," Nason said. "In Latin America you don't have the same assumption that they have a right to be protected just because they have joined the electronic age."

MIDDLE CLASS RISK

Nason says Latin America's emerging middle class is at the greatest risk for fraud, especially those whose cards have high daily spending limits.

"The upper class would have American Express cards and debit cards on U.S. banks that they would use for travel. Those cards would be protected with a \$1,000 limit per day," Nason said.

"You'll see more debit cards coming out in Latin America," which will reduce the damage from fraud because they contain a finite amount of money.

Nason, like Price, does not believe credit card fraud is acute enough to make a significant difference in the way business is done. However, others point out how economic damage can be done.

"From a business standpoint, let's say from a U.S. view, you're going to have loss of confidence in the economic infrastructure in a particular country, because it's a pervasive problem as it is at this moment," said Marta Alfonso, a certified public accountant and partner at Morrison Brown Argiz & Farra.

"If they don't get it under control, it becomes a very expensive cost of doing business. So it's not just the cost of the credit card, it's those other factors, particularly the one that deals with loss of goodwill or franchise value to both the financial institution and the merchant."

So what can a financial institution do to try to prevent this kind of fraud?

"I look at it in terms of what I call the three Ps: People, products and processes," Alfonso said.

"On the people side, you want to do some type of screening with employees and contractors working with the customers, access to the data, distribution of the processing technology, the payment card technology or securing data," Alfonso said. "Why that's really important is because at any component of that cycle there's an opportunity to skim information right off."

FOCUS ON PEOPLE

Managing that involves both training and awareness up front that tells people what their responsibilities are, that others will be watching, and there will be consequences for wrongdoing.

"For example, you normally wouldn't send somebody out to check how the processing technology is being installed," Alfonso said. "You send a provider out, he puts in a little card swipe machine and he walks away. You may have to come back and actually test check that to make sure that there isn't skimming going on."

Other solutions include data encryption, dealing with data storage and backup systems that are secure both on site and off site, masking credit card numbers in systems so that people can't see the full number and security logging and monitoring. Behavioral software allows monitoring for activities to identify anomalies like

randomly assigned IP addresses, serial credit card transactions from the same card, unusual geographic patterns or concentrations of charges. Other red flags include orders to a single address with multiple cards or orders being shipped to post office boxes.

"In those cases you acquire additional authentication for certain types of transactions where you require them to fax you back ID or additional authentication," Alfonso said.

Data clearinghouses can be established to deal with address and card verification and both payer and bank authentication, Alfonso said.

TRAVEL ALERT

One example increasingly familiar to North American consumers is that credit cards cannot be used internationally unless the bank has been made aware the cardholder is traveling abroad.

"That calls for customer training and awareness on accounts and monitoring patterns of transactions, where you have the opportunity, for example, to contact a customer," Alfonso said. "You might decide in a bank that your policy is for any purchase over \$500 that you're going to call the customer back and confirm it. You can have people there to do that."

Banks can also retain internal histories of customers to spot repeat offenders and share that information with multiple financial institutions.

"You can't use remote or mobile PCs in the processing center, no wireless and then make sure that everything is encrypted, there is secure backup, that you shred documentation. These can all be put in place in institutions that have lower technology budgets.

The technology, however, is only as effective as the people using it.

"The equipment is of the same caliber that you would find in the United States, it is that the level of experience and the time commitment given the exploding growth," Gutierrez said. "It's a resource allocation issue ... to implement systems that catch things."

Price agrees that the low-tech crimes occurring in Latin America can be rooted out with low-tech solutions.

Price said that while the back-and-forth battles between hackers and computer security professionals are often beyond the comprehension of card industry executives, they do have an arsenal of low tech weapons at their disposal.

Background checks of employees and vendors, especially those handling sensitive data, and audited IT security, will expose many internal sources of fraud, he said. And in any case, he notes, high tech defenses alone are not enough to beat low-tech crime.

Harper's prediction for the region is optimistic.

"If credit card theft here is on its way down, it will also be on its way down there, as they become more sophisticated with the due diligence, honest employees and internal checks and balances," he said.

Wayne Tompkins can be reached at (305) 347-6645.