



Could growing ATM fraud accelerate US conversion to the chip card?

Could growing ATM fraud accelerate US conversion to the chip card?

Contents

- 3 Introduction**
- 4 The Rise of ATM fraud**
- 5 Beating the fraudsters**
- 8 A better way to tackle ATM fraud**
- 10 About Level Four Americas**

Could growing ATM fraud accelerate US conversion to the chip card?



Introduction

The real cost of ATM fraud in the US is approaching \$200 million a year and rapidly increasing, despite industry efforts to improve security and customer education.

Smarter criminals work on a larger scale using the latest technology. Other regions of the world are replacing magnetic stripe payment cards to address this rising tide of fraud. Perhaps the US should consider introducing chip cards into its ATM networks before the situation gets out of control.

ATM fraud has become much more sophisticated over the years. Aside from 'shoulder surfing', mugging and forced withdrawals, criminals have embraced more subtle electronic means of perpetrating their fraud.

Vulnerable ATM networks

The criminal community has historically focused its efforts on the fraudulent use of credit cards at point of sale (POS) for a number of reasons. Magnetic stripe cards are easy to counterfeit so stolen cards can be used directly because signature identification is simple to fake. More importantly, the global network makes it easy to execute the fraud internationally. High credit limits make credit cards an attractive target, even if the purchased goods then have to be sold on to convert to cash.

But technology, such as neural networks for analytics, and administrative measures has borne down on credit card fraud at point of sale. And especially in countries where POS terminals are always connected to online networks for authentication of transactions, this kind of fraud has been reduced to manageable levels.

This has forced criminals to explore other opportunities for card fraud. These include card not present transactions, a type of fraud assisted by the growth of the internet as a channel for the financial services and retail industries, and ATM fraud, which is growing rapidly worldwide as professional criminals have realized the vulnerability of ATM networks.

ATM fraud has become much more sophisticated over the years. Aside from 'shoulder surfing', mugging and forced withdrawals, criminals have embraced more subtle electronic means of perpetrating their fraud.

According to analytics company Fair Isaac, the first 'Lebanese loop' devices, which are used to trap cards and money in the machine, began to be used in 1994. This was followed by the first reports of externally compromised ATMs in 1998. In recent years there have been a growing number of instances of machines owned by independent sales organizations (ISO) being internally compromised, and also a growing number of external skimming and video devices being used to capture magnetic stripe data and customer's PINs.

Technology is now readily available that allows the criminal to 'skim', or copy, the magnetic stripe as it is inserted in to the ATM card reader. The PIN can be recorded with a miniaturized camera, or with an overlay on top of the real PIN pad that does not interfere with its function. The card and PIN information can be transmitted to the criminal in a nearby van and a counterfeit blank card produced in minutes. This can then be used safely to withdraw cash without the customers' knowledge until the fraud is detected either by the customer spotting illegal withdrawals on his account, or the bank registering that a particular ATM has been compromised.

Whether the card reading and PIN capture have been wired internally or attached externally, both these types of modification are much more sophisticated than- the earlier Lebanese loop and other front panel 'ghost' modifications for card detail and PIN capture. In most cases the cardholder's suspicions will not be aroused, and the criminal has much more time to withdraw cash until funds run out or the card is cancelled.

Could growing ATM fraud accelerate US conversion to the chip card?



Beating the fraudsters

Rapid growth in fraud

Fraud attacks on ATM networks is of particular concern in the US, where the growth in third-party managed ATMs networks through independent sales organizations (ISO) provides soft targets for criminals. ATM fraud in the US has grown rapidly in the last few years, and now stands at around \$50 million a year according to estimates by the Electronic Funds Transfer Association (EFTA). ATM fraud has continued to rise globally in 2004, with growth rates in excess of 35 percent in some countries.

ATM fraud is growing because it produces cash and is fairly low risk to commit. If equipment is compromised, the criminal just drives away. It is then almost impossible to identify criminal when they withdraw cash on video surveillance if they take rudimentary precautions. The equipment required can also be easily acquired in large volumes without being tracked. Off the shelf miniaturized cameras, transmitters and simple card skimmers are readily available and cheap, despite the efforts of US Customs to crack down on their import.

ATM fraud also lends itself to structured organized crime gangs, as there are plenty of expendable 'junior lieutenants' to perpetrate the crime. They can quickly spread out across a city with multiple cards to withdraw a huge amount of low value transactions. The fraud is repeatable and very profitable, and there have been reports of international criminal gangs 'franchising' the necessary equipment to the underworld.

The complex structure of the US industry, with many ISOs and different acquirers and network operators has made it a challenge for industry bodies, such as the ATM Industry Association (ATMIA), to implement a response.

But the most pressing concern for the US banking industry is that while ATM fraud is a global problem, most major world economies except the US are moving to embrace EMV-standard smart chip cards in their ATM and POS networks. Chip cards radically reduce card counterfeiting and counter the most damaging types of fraud being perpetrated today, due to the complexity of the chip itself and the information it holds. Chip cards also provide a platform for offering value added applications on top of the payment functionality on the cards.

ATM fraud in the US has grown rapidly in the last few years, and now stands at around \$50 million a year...

The US, despite pressure from the cards networks, has not joined the initial migration to the EMV standard. This is mainly because of the massive cost of upgrading the national POS infrastructure, and the fact that fraud at point of sale is not at a high enough level to justify the massive investment required in hardware, training of retailers and re-education of customers. ATM fraud levels alone also do not justify migrating the whole country's ATM and POS networks in tandem to support chip cards. But there is a sound argument for starting to first upgrade just the ATM network to support EMV.

From January 2005, in the case of Western Europe and some countries in Asia Pacific, or from January 2006 for the rest of Europe, the Middle East, Latin America and Canada, most countries are looking to tackle card fraud through the use of EMV standard chip cards. The introduction of chip cards removes the main point of weakness in today's infrastructure - the magnetic stripe card, which is incredibly cheap and easy to duplicate.

As the rest of the world moves away from magnetic stripe cards to chip cards, organized criminal gangs are likely to focus more attention on the US, the world's largest economy, which is still reliant on the vulnerable magnetic stripe. This fraud migration will quickly become apparent as North America's more immediate neighbors, such as Latin America and Canada, migrate to EMV.

Many customers affected

The average amount that can be defrauded from any one ATM debit card customer is relatively small when compared to many instances of credit card fraud. In the one case of an organized gang that compromised around 60 ISO machines between 2001 and 2003, cards and PINs were replicated for 21,000 accounts for a total take of around \$3.75m. Although some people would have lost much more, the average loss suffered by each bank customer was just \$178.

Taking this average figure and applying it to the \$50 million in ATM fraud perpetrated in the US in 2003 reveals that approximately 281,000 customers were affected. This is a large number of customer enquiries and investigation and reparation processes to go through, not to mention a large number of customers who are having unfavorable experiences with their banks. The process cost involved, often not tracked or released by banks, means that the growing annual ATM fraud figure hides a much larger problem. A study by HNC Card Alert Services in 1995 estimated total costs at four times the direct fraud losses involved.

Leaving aside the adverse impacts in loss of consumer confidence and negative publicity, which are harder to quantify but real nevertheless, we can assume that total cost to the banking industry from ATM fraud is approaching \$200 million per year and rising.

Could growing ATM fraud accelerate US conversion to the chip card?



This growth is likely to continue in the next few years, despite current efforts to foil skimming attacks and improve operational security practices. This includes changes to the process of being sponsored onto the inter-bank network and becoming an ISO. These changes introduce more stringent background checks on applicants and are designed to minimize the risk of criminals plugging their own internally modified ATMs into the banking network.

These moves have had mixed levels of success. As demonstrated by an NBC Dateline report of December 2003, convicted fraudsters were still able to get into the ISO business without going through background checks. Optimistically, the new stricter guidelines were just taking time to filter down into daily practice at the time of this report. But a more pessimistic view might be that there are still ways and means of getting into the ATM provision business with malevolent intent.

Other measures being promoted by organizations such as the ATMA's Global ATM Security Alliance (GASA) include best practices for: the video surveillance of ATM users; regular inspections of the equipment by bank staff; and customer education to encourage them to report odd equipment and shield the PIN pad during use.

Many banks are also lowering daily cash withdrawal limits to minimize their exposure to risk, even though this has more of an impact on customer convenience than fraud vulnerability. And the ATM manufacturers have responded to the threat by incorporating improved designs for new models and offering new modules for existing machines.

Low-cost devices that can provide a temporary fix include a 'jitter' card reader that moves bankcards sideways slightly as they are swiped to make it hard for skimming devices to read data off the card. Another is a simple piece of plastic that sits around the card reader to make skimming devices harder to put in. Some manufacturers are also promoting new capabilities for their latest models, which can detect when the reader or PIN pad have been tampered with and de-activate the machine.

The process cost involved, often not tracked or released by banks, means that the growing annual ATM fraud figure hides a much larger problem.

The fundamental problem is that the magnetic stripe is not secure.

Half measures

These measures are only partially successful for a number of reasons. The criminal is always aware of video surveillance and can take the necessary precautions such as hiding their appearance when making withdrawals, and subtle and rapid attachment of scanning equipment. Thanks to the ISOs, ATMs are now sited in a much broader range of locations, which make video surveillance and regular checks more difficult. Criminals are aware of this, and often focus on the 'soft target' ATM in a deli or bar.

But this does not mean bank-wall ATMs are safe. Often, because of the higher volume of customers, criminals will attack a busy main-street ATM in the hope of capturing a large number of accounts in a short time. And while newer ATM equipment can make the attachment of skimming devices more difficult, the US has a large number of legacy machines, at banks and ISO locations, which are vulnerable.

Whether it's an ISO or bank ATM, customers are still not sure what they are looking for when it comes to compromised machines, and a lot of the externally attached equipment is high quality and extremely subtle. There is also a wide variety in ATM models, which makes customer vigilance fairly ineffective. Customers are also lazy and well entrenched in the way they use machines and are usually do not cover the PIN pad sufficiently to completely obscure a camera.

Current customer education campaigns might have some success in getting people to remember what their most commonly used ATMs are supposed to look like, and be more aware of the potential for skimming modification. But the whole point of ATMs is that they are everywhere you go, and people will continue to use different ATMs depending on their activities.

Attacking the problem at the source

Most US banks are already well on the way to upgrading all their ATM estates to TripleDES encryption and encrypted PIN pads to meet the deadline imposed by the card schemes of April or December 2005 (some larger networks negotiated a more lenient deadline). This will address the problem of internally compromised ATMs, but the biggest vulnerability remains the ease with which external equipment can be used to compromise an ATM.

The fundamental problem is that the magnetic stripe is not secure. It is too easy to duplicate, and any initiative that does not address this weakness is just a band-aid on an open wound. And open wounds are prone to infection.

As the chip card closes the door on ATM fraud in most parts of the developed world, the focus of the international criminal will turn to the remaining relatively unprotected magnetic stripe ATM networks in the US. Throughout 2005 and 2006 this is likely to result in a huge growth in the volume and value of attacks.

Could growing ATM fraud accelerate US conversion to the chip card?



The obvious solution to the problem is to upgrade the ATM infrastructure to support EMV chip cards. This does not have to be linked into an upgrade to the POS infrastructure and does not need to be linked to a migration deadline agreed with the card schemes.

Because it's the card issuers and not the ATM acquirers that actually pay for the fraud, there would likely be push back from many ISOs and acquirers about investing in upgrades required for chip card support. But banks who do commit to protecting their customers from fraud on their own ATMs could gain significant competitive differentiation, and may be able to put pressure on any ISOs they sponsor to follow suit.

A phased introduction of chip-cards and support in ATMs across a bank's customer base and network could have a major impact on reducing the up-front and operational costs of fraud. But gradually introducing support for chip cards could also have other benefits.

From a banking industry perspective, it could ease some external pressures. Moving towards embracing the EMV standard, if only the ATM network at first, would go some way to easing the pressure on the US banking industry from the card schemes, which are very interested in seeing global compliance.

And also, with the rest of the world embracing chip card technology, there will likely be pressures on tourism with card compatibility. People traveling from Europe and Asia Pacific often expect to encounter card and network incompatibility problems when they are traveling in less developed countries. But traveling to the world's largest economy they do not expect to encounter a higher risk of fraud when withdrawing their holiday spending money.

Some banks in the US have already been undergoing trials with chip cards, but this has not been security driven. Rather, they are interested in the multi-application potential for the cards in delivering value-added services. This can be in the form of stored value ticketing systems for public transport, or loyalty programs and other business initiatives that banks can enter into with the retail and entertainment industries to leverage the card real estate

Adding the potential for competitive differentiation through such services to the fraud-reduction capability of EMV further strengthens the business case for US banks to begin moving to chip cards for their ATM networks.

Could growing ATM fraud accelerate US conversion to the chip card?



About Level Four Americas

About Level Four Americas

Level Four Americas provides best-of-breed ATM test and development software to retail banks and ATM manufacturers. It is the sister company to Level Four Software, the leading provider of ATM test and development in Europe and the Middle East. Level Four Americas was founded in September 2004 to provide Level Four's tools to North America, Latin America and the Caribbean.

Since 1995, Level Four Software has been working with leading financial institutions to unlock the profit potential of their ATM delivery channels. Level Four's key offering is the ATM Channel Development Suite, a comprehensive suite of integrated modules that enable rapid development of new ATM applications and full end-to-end testing of ATM networks. By providing software solutions with measurable economic benefit to its customers, Level Four has built an impressive customer base including Royal Bank of Scotland, Abbey, Nationwide and Woolwich. Level Four partners with key players in the ATM and payments arena including ACI, Diebold, NCR and VISA to provide complete integrated solutions. Level Four has offices in Dunfermline, Scotland and in London. Visit Level Four on the web at www.levelfour.com

Could growing ATM fraud accelerate US conversion to the chip card?



Level Four Americas
Coral Way, Suite 308
Miami, Florida, USA
FL 33145

Telephone:
1.305.385.3000

Facsimile:
1.305.388.3007

Email:
americas@levelfour.com

Internet:
www.levelfour.com/americas

The information in this document
is subject to change without notice.

© Copyright Level Four Software Ltd.
2004. All rights reserved. Reproduction,
adaptation or translation without prior
permission is prohibited except as allowed
under copyright laws.

Produced by Level Four Software Ltd
in the UK 11/04.