2007

The Phantasm of ATM Withdrawal

Nattakant Utakrit
Edith Cowan University

DOI: 10.4225/75/57b55313b8763
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

The Phantasm of ATM Withdrawal

Nattakant Utakrit
School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
nattakau@student.ecu.edu.au

Abstract

Despite the stringent legislation and increased enforcement aimed at combating financial crime, fraud using cash machines remains a public concern. The problem of ATM fraud is happening on a global scale and the ramifications have been felt in Australia. This paper highlights the stratagems of financial crime, in particular of ATM fraud. The abuse of ATMs with intelligent methods used by perpetrators will be discussed. At the same time, the paper will present some global cases of ATM fraud. Finally this paper will illustrate countermeasures and security methods, such as biometrics and premises protections of banks, financial institutions and customers, to mitigate crimes.

Keywords

Automated Teller Machine (ATM), fraud, Lebanese Loop, skimming, counterfeit, Personal Identification Number (PIN), biometrics

INTRODUCTION

Automated teller machines or ATMs are widely used these days. They make financial transactions of cardholders easier. People do not need to carry a lot of money with them all the time because there are electronic machines available to facilitate transactions whenever they want in most public areas. However, the use of ATMs can bring problems for the cardholders and financial institutions when skimmers take advantage of unsuspecting cardholders. Financial crime, especially ATM fraud and identity theft, is now a serious issue which is continuously on the increase. Financial crime has a big impact on the global economy. In one year, financial crime cost the economy about $60 million US, and this did not include the identity fraud which was $625 million US annually (Cato, 2007). This paper considers reasons why ATM fraud is becoming more targeted and the different attacks toward ATM cardholders.

ATM and the facilitation

In the past, ATMs were designed so users could only take cash out. This capability did not make ATMs successful worldwide because the risk of holding cash was high. People could get attacked when they held cash. Would it not be better if the ATM machine could be a contactless payment station? Therefore, financial institutions are now trying to improve the payment method through ATM facilities. The latest functions from ATM machine can operate in the different purposes such as depositing checks, accepting payments, paying bills, offering advertising, dispensing tickets, topping up contactless payment devices or even downloading back statements to PDAs (Kitten, 2007). Nevertheless, the updated technologies could bring higher risk to cardholders.

STRATAGEMS OF ATM CARD FRAUD

The strategy of ATM fraud is getting more complicated and technical in nature. Many unsuspecting customers are victimized by skimmers without any warning. Basically, criminals have common ways to take money and obtain personal details from customers by both low- and high-level technical abuse. The methods that criminals usually use are shown below.

Lebanese Loop

This technique is well known in criminal financial fraud reports. Lebanese loop is a skimming method in which a plastic envelope is designed to block the hole in the machine perfectly (Mikkelson, 2006). When the card is inserted, the machine will not be able to read the card even if the PIN numbers is keyed in correctly many times. At this stage, the skimmers will pretend to be an innocent assistant and try to help the victim by asking that person to input the PIN numbers again and again or they will offer help in retrieving the card. Eventually, the victim will give up and walk off without the card. The skimmers will wait patiently until they are certain that the

victim will not return. Then they pull the plastic envelope out and take the card away with the memorized PIN numbers. The case below is one of such example claimed by Mikkelson (2006); which happened to a lady in HSBC at Hanover Square on Saint George Street where the ATM machine failed to return her card. She thought she could come back in the early morning to take the card out, but the card was not there when she arrived.

Recently, the Lebanese loop was introduced with the latest fraud accessory which is made from a thin and clear rigid plastic 'sleeve' such as the x-ray film and cut it to the size of the slot machine (Cottrell, 2007) in order to prevent the machine from reading data. The data will be scanned and encoded at the magnetic strip from the back of the card. Thus, the machine will require the customer to re-pin the PIN numbers again and again. At the time, the skimmer will come along and offer to help the customer (Mikkelson, 2006).

In another variation of Lebanese loop, the obstructing material can be made from a length of tape which is inserted into the card slot so that the card can be trapped and fail to return to the customers (North East Fraud Forum, n.d.). In the end, the criminals will continue their duty as a kind assistant as described above. Figure 1 shows how the tape may be set up. To protect customers from Lebanese loop attacks, checking the ATM machine before the card is inserted is an appropriate way to proceed. Mikkelson (2006) suggested that it is possible to identify a Lebanese loop attack by thrusting a finger inside the card slot before the card is inserted. The users can feel if there is a sleeve with a couple of tiny prongs inside the slot machine to help the thieves get the sleeve out of the slot when they want to take the card.

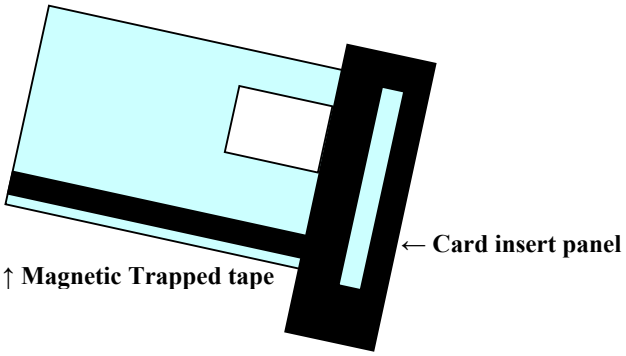

Figure 1. A tape inserted inside the card slot

A counterfeit slot machine

This method is described as a criminal act in which the original card slot is covered with a similar forged one. The spurious card slot will skim the ATM card number and card details from the magnetic strip on the back of the card ("ATM Camera", n.d.). The skimmers, who usually sit inside a car in a nearby car park, will receive the data from the equipment they installed on the front of the ATM machine ("ATM Scam", 2006). Mckinnon (2007) claimed, from Patton's concept in the Knight Ridder Tribune Business News, that those thieves can sell the collected information either by data scanning through the nearby receiving machine or data encoding with the duplicate cards. The new duplicated card can be a plain white card, plastic card or telephone card which is able to store encoded data. (North East Fraud Forum, n.d.). Also, the issue about ATM Advice - How to protect your card details (n.d.) in North East Fraud Forum website describes how the forged ATM card works after the data is captured. Once the card information is trapped, the perpetrators will list the numbers and the correct pin numbers (usually it will be kept in a book) and take out the maximum amount of cash within the next hour or the next morning. Nevertheless, it is not normally difficult to identity a suspect machine even though the colour, shape, and material are designed to imitate the genuine one. However, if any part of the machine is convex or looks unusual, one can assume that the machine has been compromised.

Leaflet holder captured

This technique is committed by embedding a minute wireless camera inside the leaflet box close to the keypad and screen. The hidden camera will capture and monitor when customers key their PIN. The effective camera can transmit the image to the nearby receiver up to 200 metres away ("ATM Camera", n.d.). This technique has been utilised in Bradesco, a Brazilian bank, where the criminal wanted to steal information and money from the bank customers ("ATM Camera", n.d.). See Figure 2 for a diagrammatic representation.

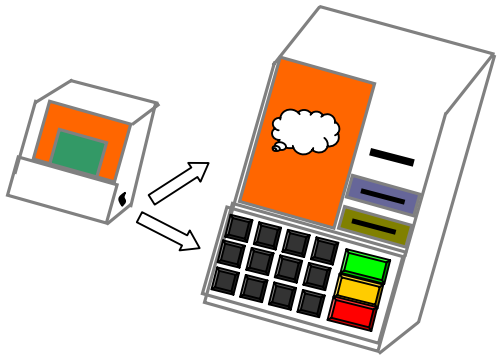

Figure2. The angled view of the wireless camera in the leaflet box

Hidden Camera in a Fake Top Panel

This method is very similar to leaflet holder capture, but the position is different. The minute and thin camera which is around 7 cm high ("ATM Camera", n.d.), will be hidden inside a fake panel embedded at the top of the ATM casing. It is hard for people to see as the color and texture of the fake panel are very similar to the real one. The camera is used to captured the PIN entry on the keypad ("ATM Camera", n.d.). Inside the camera, there will be a transmitter which is the same as the device found in door bell chimes. This device will transmit the actions of a customer entering a pin number to a nearby receiver which could be up to 300 metres away from the cash point (North East Fraud Forum, n.d.) This technique has been used in Hong Kong (January 2004) where, as an example, the camera was hidden inside the ATM machine of the Hang Send Bank branch in Tsuen Wan ("ATM Camera", n.d.).

Shoulder surfing

Obviously, card-skimming can be accomplished through a low-tech method such as shoulder surfing. In this simple technique, skimmers usually stand behind the victim and try to look over the victim's shoulder to view the PIN. They might also listen to the sound of keystroke PIN pad and memorize it to commit the card fraud or card theft (Bidwell, 2002). There is easy way to notice skimmers in that the suspicious person will stand too close or stand in an angled position beside the person who is taking the money out of the machine.

Captured plastic skimmer

Another obvious card skimming device is called a keystroke captured skimmer. It is a thin and transparent plastic film with the recording microchips underneath the device; which is overlaid on the top of the ATM keypad and looks like a normal plastic cover. The texture of the keypad will be smooth and greasy. It is used to capture the keystroke when customers press the PIN numbers (Richard, n.d.). This plastic misleads customers that it is a new used keypad or it is used to cover the dust or cover the printed number keypad not to fade too early. Some ATM machines are covered with the fake keypad cover which is similar to the original one. It makes the keypad higher than the normal one. See Figure 3 for a diagrammatic representation.

Other skimmers

It is wrong to think that ATM fraud can happen only with withdrawal machines. In fact, there is a risk of ATM fraud happening inside shops such as restaurants, kiosks, and convenience stores. These point-of-sale outlets may be operated or be compromised, by card skimmers or fraudulent employees. It is possible to install a counterfeit hand-held card reader to capture the PINs. When customers press their identification codes on the machine, the device will capture the data and transmit it to another receiver machine nearby (Richard, n.d.). Another case, the forged hand-held card reader could send an error message or fail to operate on the hand-held screen after customers press their PINs. Crooked employees may ask customers to re-do the transaction again with the real device after that. This may not be noticeable because most customers seem to trust point-of-sale systems.

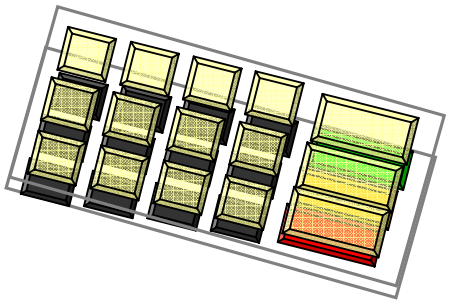

Figure 3. A captured plastic cover is designed to mislead customers

AUTOMATED TELLER MACHINE ABUSE

What should we know about data skimming? What will happen with the skimmed data? Once the data is installed in the skimmer device and transmitted to a computer, the data is then recorded onto another counterfeit card which is made similar to the original one. The counterfeit card must have a magnetic strip at the back so that the data can be installed. This type of card can be found in general use such as a library card, a security card or even a parking ticket (The Model Criminal Code Officers' Committee, 2006).

It does not take too long for criminals to get money out of the bank as long as they can get either or both ATM cards and PIN numbers. Usually, data on the counterfeit card is likely to be used to withdraw cash from ATMs rather than to purchase products at point-of-sales counters. It is often too obvious and easy to get caught when skimmers attempt to buy something with the forged card (The Model Criminal Code Officers' Committee, February 2006). Thus, the skimmers use equipment to copy the card and to use the PIN numbers to withdraw the maximum amount of money from the ATM before the real holder deactivates the card ("ATM Camera", n.d.). These criminals almost always use the fake cards to withdraw the money in other cities in the hope of avoiding detection by the police (Cato, 2007).

After the authorized customers find that their money has been stolen, of course they must deactivate their card and freeze their account to protect it from further theft. Nevertheless, by the time they realize that there might be something wrong with their card; they have probably lost all of the money in the account. Most interestingly, it has been found that the incidence of card skimming has increased to the point where it is of serious concern in Australia. Skimmed details are transmitted to other countries, where data is added to forged cards and sold to tourists to spend (The Model Criminal Code Officers' Committee, February 2006).

COUNTERMEASURES BY BANKS AND FINANCIAL INSTITUTIONS

Banks and financial institutions are trying to develop intensive ATM fraud countermeasures in order to protect their assets, finances, and their customers' assets and financial wellbeing. Countermeasures may be divided into two types of security protection, those for:

- banks and financial institutions' assets, and
- banks and financial institutions' customers' assets.

Banks and financial institutions' assets

Banks and financial institutions' properties cannot be modified, manipulated or destroyed if the banks are to protect their reputations and credibility for their users. These methods are being used to protect the financial institutions' properties:

27. Installing a jitter mechanism, a detective sensor, to prevent skimming. A vibration technology is used to protect the data on cards against being read accurately by fake card readers ("Diebold Launches First-of-Its-Kind, Consumer ATM Security Web Site", 2005)
28. Installing vigilant detective systems ("Diebold Launches First-of-Its-Kind, Consumer ATM Security Web Site", 2005). These systems report when any suspicious skimming devices are installed; they will transmit signals to alert the financial institution to stop processing transactions and/or close down the ATM.

29. Installing camera surveillance to record all activities within the area surrounding the ATM.
30. Installing deep and recessed screens, and keypads, to shield customers from shoulder surfing ("Diebold Launches First-of-Its-Kind, Consumer ATM Security Web Site", 2005).

Banks and financial institutions' customers' assets

Many ATMs are not located inside bank offices. The objective of this protection is to guard customers from being physically attacked when they are doing their ATM transactions and when they are carrying the cash they have withdrawn. These are some of the good techniques that being used to protect customers:

31. Installing mirrors to allow customers to watch what is happening behind their backs and in the surrounding area.
32. Installing various lighting options around the cash machine and in nearby car parks where suspicious persons may be hiding (Diebold, n.d.).
33. Installing video surveillance around the premises ("Diebold Launches First-of-Its-Kind, Consumer ATM Security Web Site", 2005).
34. Posters or secured warning signs should be posted around the ATM machine to warn people of possible dangers.
35. Designing rounded fascias for slot machines to prevent skimmers from installing skimming equipment easily (Diebold, n.d.).

The concept of lobby or vestibule banking (Slater, 1991) seems to be the best way to deter crime. Many ATMs have been located within banks' doorways, or close to kiosks protecting ATMs. Installing a protective glass screen around the existing dispenser offers customers some protections while their withdrawals are being processed. Cash and card robbery may be reduced as a result (Slater, 1991). Using the customers' ATM cards and PINs as means of controlling access to cash points may also increase customer confidence.

Biometric protection

The issue of biometric protection has been discussed frequently. Would it not be better if customers walked to the bank without having to memorise passwords and carry proof of identity? Biometric identification allows customers to make financial transactions securely. Biometric techniques may involve fingerprint scans, validation of skin texture, iris scans, retina pattern scans and face recognition in addition to signature verification (Shah, 2001).

It is one of the most effective security methods used worldwide. For example, in India various biometric techniques have already been implemented (Shah, 2001). They represent identity checks which cannot be falsified, by using a physical or behavioural characteristic to verify personal authenticity. Biometrics can be divided into physiometric and behavioural techniques (Hendry, 2001) as is shown in Table 1.

Table 1: Types of biometric protection

Biometrical types	**Biometrical acts**	**Identification acts**	**Possible exceptions?**
Behavioural	Signature verification	The relative speed and the pressure used by the writer may be consistent.	Depends on the writing surface, the environment, mood of the user and writing tools.
Behavioural	Keystroke dynamics	Skilled typists	The diversity of keyboards and the software used might lead to error.
Behavioural	Voice recognition	Multilevel voice checking such as tone, pitch, and cadence.	False rejection may happen with unusual background noise, colds or influenza, and mood of the user.
Physiometric	Hand geometry	Captures the pattern of palm lines on the hands	Injury, aging, out of date devices may affect the measurement.

Physiometric	Iris scan	Measures the flecks in the iris of the eye.	Those in wheelchairs and or those who are very short may experience difficulty.
Physiometric	Retina scan	Estimates the characteristic blood vessel patterns on the retina with a lower-power infrared laser and camera.	Eye disease can destroy the gene or tissues which will have an impact on the accuracy of the retina scan measurement.
Physiometric	Finger/Thumbprint	Captures the minute detail of individual fingerprints.	Analysis may be difficult for those who are heavy smokers or work in some trade where the work is dirty or repetitive.

Source: Modified from Hendry, 2001.

Furthermore, modern technology may be used to create new security measurements to detect and monitor card users' activities. For example, anti-fraud software is used to monitor all spending and financial activities and to track unusual transactions, even when the card has been used from one region to another in a distant country (Richard, n.d.).

CUSTOMER DEFENSIVE ACTS

Customer defensive acts are low-tech methods which may be used to enhance personal security and to avoid being defrauded by ATM scams. There are many simple methods to apply:

36. Caution and vigilance should be taken when using cards. If there is anything suspicious about the machine, the customer must contact the bank to report the issue or to ask why changes to the machine were made (Richard, n.d.).
37. PIN entry should be shielded from prying eyes. Customers should protect their PIN numbers by standing close to the ATM, by covering the PIN keypad and ensuring that it has been blocked from shoulder surfing (North East Fraud Forum, n.d.).
38. The environment around should be clear. Try to avoid using an ATM when people stay close to the machine. Ask them to move aside politely if it is possible or find another ATM somewhere else (Mikkelson, 2006).
39. Using ATMs in secluded areas should be avoided. It is safer for customers to have friends accompanying them if it is necessary.
40. Everyone should beware of the helpful stranger. Do not trust anyone offering help especially if the card is stuck inside. Report the incident to the bank and deactivate the card as soon as possible (Mikkelson, 2006).
41. Move to a safe distance before making the phone call to report a stuck card. The card should not be removed as it may be used as evidence (An Garda Síochána - Ireland's National Police Service, n.d.)
42. Expensive jewelry and valuable items should not be worn or carried ("Diebold Launches First-of-Its-Kind, Consumer ATM Security Web Site", 2005).
43. Count the money only when it is safe to do so ("Diebold Launches First-of-Its-Kind, Consumer ATM Security Web Site", 2005).
44. Writing the PIN on the card or carrying in the wallet should be avoided. It would be better if the PIN is memorized as soon as possible (Pentagon Federal Credit Union, 2007).
45. Creating PINs should be considered carefully. Dates of birth, social security numbers, telephone numbers, account numbers, street addresses are all unsafe for use as PINs (Pentagon Federal Credit Union, 2007).
46. ATM receipts should not be left at the machine or in the nearby rubbish. Attackers might use the receipt for their own benefit.
47. Reviewing the statement balance should be performed regularly to ensure that everything is accurate (Pentagon Federal Credit Union, 2007).

48. Deactivate cards as soon as they are stolen as well as destroying old cards when new cards become available.

CONCLUSION

ATMs are very widely used and very convenient. People use ATMs for a variety of purposes, but mainly for cash withdrawal. On the other hand, ATMs may cause serious problems for users. ATM cards are possibly the most susceptible to criminal attack. Skimmers are also able to abuse the advantages associated with ATM devices for their own benefit. Their techniques are becoming more sophisticated as the technology they attack advances. However, simple methods are still being used to rip off incautious victims. Therefore, banks and financial institutions are developing software and security methods to detect, deter, and delay skimmers as well as protecting their properties, reputation and customers. At the same time, customers should endeavour to protect themselves from the risk of theft by skimming.

REFERENCES

An Garda Síochána - Ireland's National Police Service. (n.d.). *Crime Prevention Advice - ATM (Cash Machine) Fraud*. Retrieved September 29, 2007, from http://www.garda.ie/angarda/crimeprev/cadvice_atm.html

ATM Camera. (n.d.). Retrieved October 4, 2007, from http://www.snopes.com/fraud/atm/atmcamera.asp

ATM Scam. (2006). *Bank ATMs converted to steal bank customer IDs* Retrieved September 28, 2007, from http://www.utexas.edu/police/alerts/atm_scam/

Bidwell, T. (2002). *Hack Proofing Your Identity In the Information Age*. Rockland, MA: Syngress Publishing, Inc.

Cato, J. (2007). 2 illegals indicted in ATM fraud in Western Pa. *Knight Ridder Tribune Business News*, 1.

Cottrell, K. (2007). Legislators move to protect ATM users // Bill will criminalize possession of velcro 'traps' used in ID theft scheme. *The Business Press*, 7.

Diebold. (n.d.). *White Paper: ATM Fraud and Security*. Retrieved October 6, 2007, from http://www.diebold.com/rd/whitepapers/atmfraud&security.pdf

Diebold Launches First-of-Its-Kind, Consumer ATM Security Web Site. (2005). *PR Newswire*, 1.

Hendry, M. (2001). *Smart Card Security and Applications Second Edition*. Norwood, MA: ArtechHouse, Inc.

Kitten, T. (2007). *Contactless and the ATM?*. Retrieved September 29, 2007, from http://www.atmmarketplace.com/article.php?id=8903&prc=19&page=37

Mckinnon, J. M. (2007). Bank card data stolen in Sylvania Township: 'Skimmers' at 2 ATMs used digital devices to glean info. *Knight Ridder Tribune Business News*, 1.

Mikkelson, B. (2006). *Lebanese Loop*. Retrieved October 3, 2007, from http://www.snopes.com/fraud/atm/lebaneseloop.asp

North East Fraud Forum. (n.d.). *ATM Advice - How to protect your card details*. Retrieved October 4, 2007, from http://www.northeastfraudforum.co.uk/atmfraud.asp

Pentagon Federal Credit Union. (2007). *Preventing Fraud: Automated Teller Machine (ATM) Fraud Protection* Retrieved October 7, 2007, from https://www.penfed.org/productsAndRates/resourceCenter/preventingFraud/atmFraud.asp

Richard, C. (n.d.). *Guard Your Card: ATM Grows More Sophisticated*. Retrieved October 4, 2007, from http://www.csmonitor.com/2003/0721/p15s01-wmcn.html

Shah, K. (2001). *ATM banking without a PIN*. Retrieved September 30, 2007, from http://www.expresscomputeronline.com/20070903/management03.shtml

Slater, K. (1991). *Information Security In Financial Services*. New York: Stockton Press.

The Model Criminal Code Officers' Committee. (February 2006). *Final Report: Model Criminal Code Chapter3 Credit Card Skimming Offences*: Commonwealth of Australia.

COPYRIGHT