Investigating ATM Frauds In Sunyani Municipality: Customer's Perspective

Isaac Kofi Nti
Department of
Electrical/Electronic
Engineering
Sunyani Technical University
Sunyani, Ghana

James Adu Ansere
Department of
Electrical/Electronic
Engineering
Sunyani Technical University,
Sunyani, Ghana

Albert Appiah
Department of
Electrical/Electronic
Engineering
Sunyani Technical University
Sunyani, Ghana

Abstract: Customers in the banking industries in Ghana have seen a tremendous change in banking activities and deliveries, since the introduction of electronic banking systems. This research seeks to examine the knowledge of Automatic Teller Machine (ATM) card and its service users, educate the general public (**Customers**) on frauds associated with ATM and how to protect themselves against these fraud. The research also outline strategies and methods that customers and custodians of the ATM can adopt for prevention of some ATM frauds. Questionnaires and semi structure interviews were used as a methodology to collect data. A non-probability sampling technique was adopted by this research to provide a range of alternative techniques based on researchers' subjective judgment. We employed Microsoft Excel and SPSS for analysis and interpretation of the collected data. ATM users of selected banks in the Sunyani Municipality were defined as population of interest. A sample size of 500 ATM users from different banks were used as a case study. The findings showed that, only 57 out of 438 representing (17.76%) of respondents that uses ATM and it service have a little knowledge about frauds associated with ATM in the municipality.

Keywords: ATM-Frauds; Skimming-Attacks; PIN-Cracking; Phishing-Attacks; Shoulder-Surfing; Cash Trapping; ATM Malware; Sunyani-Ghana

1. INTRODUCTION

The advancement in technology has made banking moved from the cash economy to cheque economy, and now advanced to plastic card economy (Twum, et al., 2016). Lately, the debit card has become the wildest emergent medium of payment around the globe (Mahony, et al., 2001). Automatic Teller Machine ATM is a cash-machine mounted by financial institutions and banks, which enables their customers and clients to perform banking services, like cash deposit, cash withdrawal, and request of mini statement, balance query and money transfer from one account to the other and also mobile money transactions for some ATMs (Twum, et al., 2016). The first Automatic Teller Machine introduced for public use was by Barclays bank in 1967, in London, Hendson branch, which had the capability of dispensing a constant amount, when its users inserts a special coded card. Since then, ATM has developed to be small in size, easier to use and faster in communication (Das & Jhunu, 2011). The introduction of the ATM into the banking industry has made available a 24 x 7 hours cash withdrawals and deposits to bank customers and clients. The ATM since its implementation has suffered numerous fraud attack and still continue to suffer these attacks.

2. ATM FRAUDS CASES

Theft in ATM machines has increased widely. The current authentication mechanism (Personal Identification Number) of the ATM machines are not safe in order to provide proper security for cash and users (Hirakawa, 2013) and (Varalakshmi, 2015). According to the European ATM Security (EAST), a total of 1,459 ATMs were raided all over

Europe in the first half of 2009, totalling 4.5 crimes or attacks annually for every 1,000 ATMs. And also 26 ATMs were robbed starting November 2007 to November 2008, totalling 18 crimes per thousand ATMs out of 1,471 ATMs in Lithuania (Dare, 2011). A report by European ATM Security Team (EAST) shows that ATM frauds by skimming attack in the first half of 2009 has risen to 24% more by the first half of 2010 (Gunn, 2010; Twum, et al., 2016). A report by (Bianchi, et al., 2010) stated that, Germany in 2009 recorded a total of two thousand fifty-eight (2,058) cases of ATM crimes, where over 100,000 ATM users were affected, which is 20% higher than ATM fraud cases in 2008 and the trend continues in 2010. In 2013 Australia recorded growth from 43.6 cents in 2012 to 48.7 cents for every \$ 1,000 spent; this is against an increase of 4% to \$624 billion on the total amount spent by Australians. While card not present fraud increased from 45% in 2008 to 72% in 2013 in Australia. At the same time, UK saw an increase in card fraud rates from 71 pence to 74 pence in every £1,000 spent. Card-not-present fraud on UK cards increased from £246.0 million to £301.1 million (APCA, 2014). Computer frauds resulting from cybercrimes and theft have become very alarming with the introduction of numerous ATM and real time online E-banking and commerce (Awuge, et al., 2012). The Ghana Commercial Bank in 2013 was hit with an ATM theft amounting to GH¢3 million (Obour, 2013). In 2015 another ATM fraud hit Ghana, two Bulgarians withdrawn money from ATMs of some banks in Ghana by cloning ATM cards of customers (Acquah, 2015). In 2016 Six Nigerians made away with millions of Cedis from VISA ATM machines in the country from over 150 ATM, which was described by bankers and security personnel as one of the

biggest ATM scams in the history of Ghana (Citibusinessnews, 2016).

This uprising of ATM frauds among the Ghanaian populates, calls for more studies on ATM users alertness and knowledge of frauds associated ATM, so as to educate ATM users and ATM operators with the view to improving ATM service quality and customer security.

2.1 Common Types of ATM Frauds

There are numerous password attacks on ATM, but in this section of this research few are described, so that the user of the ATM can understand and beware of unauthorized access or password attacks. Basically, there are three main attacks that ATMs are subject to, namely;

1. Physical attack: Brute force attack, thus applying mechanical force on the ATM machine, with the intention of getting access to cash within the safe.
2. ATM Fraud: Bank card information theft, using an unauthorized means to get access to the customer's information stored on the ATM card.
3. Software and network attack: Theft of sensitive information or controlling ATM operations from a remote distance or automatically.

These basic three ATM attacks can be split up into;

- ✓ PIN Cracking
- ✓ Skimming Attacks
- ✓ Shoulder Surfing
- ✓ Phishing Attacks
- ✓ Card Trapping
- ✓ Cash Trapping
- ✓ ATM Malware

2.1.1 Skimming Attacks

The skimming attack is the most common attack in ATM transaction. In this attack, lawbreakers take advantage of technology to make fake ATM cards by using a skimmer (a card swipe device that reads the information on ATM card). This device looks like a handheld credit card scanner and is often clipped in close proximity to or over the top of an ATM's factory installed card reader (Mandal, 2013). When a skimmer is removed from the ATM, it allows the download of personal data belonging to everyone or customers who used the ATM while the skimmer was in place. 200 ATM card information can be stored on single skimmer (Krebs, 2010). According to Rick Doten, the annual losses from ATM totalled about \$1 billion in 2008, or approximately about \$350,000 every day from the U.S. Secret Service estimation, Card skimming accounts for more than 80 percent of ATM

fraud (Krebs, 2010). In December 2009 this particular skimmer was attached to the front end of Citibank ATM in Woodland Hills, Calif. (Krebs, 2010)

2.1.2 Card Trapping

This involves, placing a device directly over or into the ATM card reader slot, which physically captures the ATM cards when inserted into it. When the user leaves the ATM without his or her card, the card is retrieved by the thieves or hackers.

Figure 1 ATM Skimming Device. (Krebs, 2010)

With this attack one ATM card is lost per attack. At every captured card, the hackers or criminals have to withdraw the whole device. Lately a newly card trapping device capable of trapping users' cards for a long time and enhance with the ability of removing trapping cards without removing the trap device have been introduced by ATM fraudsters. The common variant is well-known as the Lebanese Loop (Mohammed, 2011).

Figure. 2 ATM Card Trapping. Source (Agarwal, 2010)

2.1.3 Phishing Attacks

This is an attack on the web, where scammers aim at luring ATM users to provide their card information and PIN details of their bank card. In a typical attack, an attacker uses an email pretending as a bank and claims that user's account information is inadequate, or users' needs to update their account information to prevent the account from being closed. The user is asked to click on a link and follow the directions provided. The link however is fraudulent and leads the system user to a different website that the attacker has set up which resembles the website of the user's bank.

Figure. 3 How Phishing Attack Works. Source: cccindy.com

2.1.4 ATM Malware

This ATM attack requires an insider, such as an ATM technician who has a key to the machine, to install the malware on the ATM operating system or software. Once that has been done, the attackers could insert a control card into the machine's card reader to trigger the malware, this gives the hacker or attacker an access to control the ATM through a custom interface and the ATM's keypad (Mandal, 2013).

2.1.5 Shoulder Surfing

Shoulder surfing Attack involves direct observation of ATM's user details by the attacker, such as looking over the shoulder of the card user, to get his/her information. This attack method is very effective in getting ones information in a congested environment, because it's quite easy to stand next to someone or stretch your neck and watch as She/he fill out a form, entering a PIN number at an ATM machine (Mandal, 2013). Shoulder surfing can also be done from a remote distance with the aid of eyeglasses or other vision enhancing devices. To prevent or minimize shoulder surfing attack, it's advisable to shield the keypad with your body when using an ATM.

Figure. 4 Shoulder Surfing. (Source: www.crazylearner.org)

2.1.6 Cash Trapping

With this attack, the attackers or criminals insert a false withdrawal close up slot. The false slot causes the cash to get stuck within it, while a customer is performing a withdrawal transaction on the ATM. The customer will leave the ATM premises, thinking the machine is out of order or may go

inside the banking hall or premises to report the incident. The attackers then return to retrieve the money or notes from the ATM.

Figure. 5 Cash is trapped by the false withdrawal shutter. Source: (Agarwal, 2010)

2.1.6.1 ATM Cash Trapping Cases

On 5th March 2011, the London city police arrested two Romanian of age 23 and 25 within a flat in Harrow. These men were found in possession of cash traps, which have been used to trap customer transactions on various ATM's. (BBC , 2011). On Thursday, 31 March 2011 two men, ages 23 and 21 were arrested for allegedly trying to steal cash from bank customers by tampering with an ATM in Chingford, using a small plastic strip which causes cash ejected from the ATM to become stuck (Daniel, 2011).

2.1.7 Eavesdropping

Eavesdropping is the process of secretly listening to the private conversation of others without their consent. Spying on an ATM user and knowing his or her PIN and then obtain his or her card by any faulty means (Mohsin, et al., 2015).

Basic eavesdropping techniques are;

- ✓ Viewing victims monitor using binocular through an open window.
- ✓ Capturing people's information by installing small cameras while the information is being read.

2.1.7.1 ATM Eavesdropping Cases

Global ATM manufacturer NCR Corporation issued an alert about a card reader eavesdropping attacks, which were first identified in Europe in 2014 and are now spreading, potentially posing a risk in the U.S. (Kitten, 2015).

2.2 The Study Area

Sunyani is the capital of the Brong-Ahafo Region of Ghana. Sunyani municipality is one out of the twenty-seven (27) administrative districts in the Brong-Ahafo region. It is located between Latitudes 7° 20' N and 7° 05' N and Longitudes 2° 30' W and 2° 10' W. Fig. 1 shows the location of Sunyani Municipality on the Ghana Map (Peprah & Ayidana, 2014).

Figure 6. Map of Ghana Showing the Location of Sunyani

3. MATERIALS AND METHODS

The data was obtained mainly from clients of Barclays, GCB, NIB, Ecobank and Zenith banks in the Sunyani Metropolis. For a good research outcome, a total population sample of five hundred users of ATM were orally interviewed and also given structured questionnaire to answer, (120 Barclays bank customer, 100 GCB customers, 105 Zenith bank customers, 50 NIB bank customers and 125 Ecobank customers). The respondents were categorized into their respective educational background by using stratified sampling method, after which simple random techniques was employed to draw proportionate sample from the stratum. Out of the five hundred questionnaires distributed, 438 responded (Response Rate 87.6%). The questions were categorized into two sections. The demographic information of the respondents is acquired in the first section while the second section collects knowledge of respondents on ATM associated frauds.

4. RESULTS AND DISCUSSION

Figure 7, shows the percentage age distributions of the 438 ATM users surveyed.

Figure 7 Age distributions of surveyed subjects

The Breakdown presented in Figure 8 shows that 19 (4.11%) of the respondents have been using ATM since its introduction in Ghana while 29 (6.62%), 38 (8.68%), 111 (25.34%), 102 (23.29%), 63 (14.38%), 54 (12.33%), 23 (5.25%) of the subjects have 7, 6, 5, 4, 3, 2 and 1 year ATM experiences respectively.

Figure 8 Bar chart of number of respondents' years of ATM usage

Customers' reasons for using ATM

The response obtained shows that, there are various reasons, which included conveniences, speed, reliability and security. The responses of ATM users are shown in figure 9

Figure 9 Customers' reasons for using ATM

Speed: respondents expressed that, they spend less time with ATM transactions as compared to the human teller. The pie chart in figure 8, shows that 385 respondents representing 87.90% of the total respondents use ATM services due to the speed involved in accessing cash and other transaction from the ATM.

Convenience: customers dodging long queues in the banking halls. In the analysis of the data gathered, where customers were given multiple choices to select from, 95.89% which represents 420 out of the 438 respondents answered that, they using ATM was influenced by its convenience.

Reliability: this is associated with the 24 x 7 hours of ATM service. 48.86% of the respondents, gave reliability as the results of them using ATM services.

Security: this talks about how customers feel secured in engaging in ATM transactions. Even though 438 of respondents uses ATM service only 105 (23.97%) out of 438 express that they are stratified with the security provided in ATM.

Customers Knowledge on ATM frauds

Respondent were ask if they have heard about ATM frauds, and 73.29% representing 321 out of 438 responded yes whiles 3.38% representing 17 responded no. Figure 10 shows the outcome of the data analysis.

Figure 10 Respondents' Knowledge on what ATM fraud is

A further question was posed to respondents to whom one way or the other have have what ATM frauds is, to examine the knowledged on the various type of ATM frauds.

Table 1 Respondents' Knowledge on ATM Frauds Types

Skimming-Attacks	7
PIN-Cracking	15
Phishing-Attacks	8
Shoulder-Surfing	13
Cash Trapping	12
ATM Malware	2
Total	57

From the data analysis shown in table 1, a total of 57 respondents out of 321 respondents that new ATM fraud had knowledge of the various types of ATM frauds, representing 17.76%. This proves that a majority of ATM users have no knowledge on the types of frauds associated with ATM and its services. Shoulder-Surfing which is the common ATM fraud reordered 13 out of 75 representing.

4.1 Protections Against ATM frauds

The low responses of customers' knowledge on ATM frauds calls for education on how to prevent or secure ATM users from its associated frauds.

4.1.1 How to Avoid Credit Card Skimmers

- ✓ Be vigilant (Keep your eyes open). When you visit any ATM and it looks a little unfastened, or sticky tape remains or you suspect scratches, be wise and report to the bank or find another one. Thieves normally attach fake or imitated fronts to ATM with tape. Also try to pick around with your fingernail at the keypad to make sure that no other keypad on top of it.
- ✓ Never ever assumed that all ATM are the same or equal. Be on guard when you find yourself in another current or tourist area, because these are prime target for ATM thief. Make use the ATM within the banking hall, as opposed to one that is just outside (Heet, 2011).
- ✓ Never leave your card in an ATM, even when you are to inform the bank of a problem. Alternatively, make a call to the bank that you at the ATM and you have a problem with your card or alert the security man on duty. This will preserve your account safe and identity protected until you get help (Keith, 2013).
- ✓ Be in the habit of using the same ATM machine for your transactions, and become familiar with it and be able to identify or recognize changes to the machine (Keith, 2013).

4.1.2 Shoulder-Surfing attacks

- ✓ Stand very close to the cash machine. Always use free hand and body to shield the keypad and your body to prevent anyone eagle-eyeing your PIN and personal information.
- ✓ Always asked for help from bank staff when you performing transactions on ATM.

4.1.3 Protection against Phishing-Attacks

- ✓ Don't you ever follow any link in an email pretending to be sent by your bank, rather visit your bank website directly and log into your accounts to see if an update notice has been sent to you. These emails are almost always a phishing scam (Keith, 2013).
- ✓ Be extra care when you receive a call from someone asking for your bank details, such persons always

pretended to be calling from your bank. Try visit your bank physically for such records updates

4.1.4 PIN-Cracking

- ✓ Do away with or preferably shred your ATM receipts, balance enquiries or mini-statements when you dispose of them.
- ✓ Always change your default PIN given your by the bank.
- ✓ Don't use easily guessed PIN such as birthday, house number, phone number etc.

5. CONCLUSIONS AND RECOMMENDATIONS

In this research, we found out that 57 respondents frequently use and have knowledge on ATM out of the total 438 respondents. We observed that about 13% of the respondents had knowledge on ATM frauds. This shows that users of ATM and its services in the municipality have little or no knowledge on the various frauds associated with ATM services, making them vulnerable to ATM attacks.

The recommendations of this research could be summarized as follows:

- ✓ Since the main source of information on ATM to customers is from their respective bank, we recommend that the banks should provide education on ATM frauds to its customers in a regular processes.
- ✓ Customers should report immediately when their ATM card is trapped in the ATM machines.
- ✓ ATM services users should read more on their own about the various forms of ATM frauds mechanism to prevent themselves from being a victim.

6. ACKNOWLEDGMENTS

We offer our sincere praises and thanks to God Almighty for how far He has kept, protect and brought us faithfully in life.

7. REFERENCES

1. Acquah, N., 2015. Citifmonline. [Online] Available at: <http://citifmonline.com/2016/06/17/ghipps-blames-banks-in-bulgarian-atm-fraud-saga/> [Accessed 17 06 2016].
2. APCA, 2014. Australian payments fraud details and Data, Australia: s.n.

3. Awuge, J. et al., 2012. An Assessment of Fraud and Its Management in a Rural Banking Industry, Kumasi: Research Report Submitted To the Business Department of the Christian Service University College in Partial Fulfilment of the Requirement for the Degree of Bachelor of Business Administration.
4. BBC, 2011. News. [Online] Available at: <http://www.bbc.com/news/uk-england-london-12655833> [Accessed 7 July 2015].
5. Bianchi, A., Oakley, I. & Kwon, D. S., 2010. The secure haptic keypad: a tactile password system. s.l., ACM, pp. 1089-1092.
6. Citibusinessnews, 2016. [Online] Available at: <http://citifmonline.com/2016/07/28/six-nigerians-arrested-over-atm-scam-in-ghana-audio/> [Accessed 28 07 2016].
7. Daniel, B., 2011. [Online] Available at: http://www.guardian-series.co.uk/news/wfnews/8946110.CHINGFORD-Cash_machine_fraudsters_arrested/ [Accessed 7 July 2015].
8. Dare, T., 2011. ATM Security annual report, Nigeria: NCR.
9. Das, S. & Jhunu, D., 2011. Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. International Journal of Information and Communication Technology Research, pp. 197-203.
10. Domeher, D., Frimpong, J. M. & Appiah, T., 2014. Adoption of financial innovation in the Ghanaian banking industry. African review of Economics and Finance, VI(2), pp. 88-114.
11. Gunn, L., 2010. European ATM crime report. Technical Report 1.2, s.l.: European ATM Security Team (EAST),
12. Heet, L., 2011. creditcards. [Online] Available at: <http://www.creditcards.com/credit-card-news/8-ways-protect-against-atm-skimming-1282.php> [Accessed 24 January 2017].
13. Hirakawa, Y., 2013. Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks. International Journal of Innovation, Management and Technology, Vol. 4, No. 5, pp. 455-460.
14. Keith, 2013. 5 Clever ATM Theft Scams. [Online] Available at: <http://www.scambusters.org/atmtheft.html> [Accessed 24 January 2017].
15. Kitten, T., 2015. [Online] Available at: <http://www.bankinfosecurity.com/blogs/easy-access-fuels-atm-attacks-p-1884> [Accessed 7 July 2015].
16. Krebs, B., 2010. ATM Skimmers Part II. [Online] Available at: <http://krebsonsecurity.com/2010/02/atm-skimmers-part-ii/> [Accessed 24 June 2015].
17. Mahony, D. O., Peirce, M. & Tewari, H., 2001. Electronic Payment Systems for E-Commerce. 2nd ed. Boston, London: Artech House.
18. Mandal, S., 2013. A Review on Secured Money Transaction with Fingerprint Technique in ATM System. International Journal of Computer Science and Network, 2(4), pp. 8-11.
19. Mohammed, L. A., 2011. Use of biometrics to tackle ATM fraud. Malaysia, IACSIT Press, Kuala Lumpur, pp. 331-335.
20. Mohsin, K., Saifali, K., Sharad, O. & Dr.D.R.Kalbanded, 2015. Enhanced security for ATM machine with OTP and Facial. s.l., Elsevier B.V., pp. 390-396.
21. Obour, S. K., 2013. [Online] Available at: <http://graphic.com.gh/news/general-news/8459-gcb-confirms-money-theft-from-atm-but-says-amount-is-lower-than-gh-3-million.html>
22. Peprah, P. O. & Ayidana, H. E., 2014. Population and Housing Census, District Analytical Report Sunyani Municipality, Accra: Ghana Statistical Service.
23. Twum, F., Nti, k. & Asante, M., 2016. Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication. International Journal of Science and Engineering Applications, 5(3), pp. 126-134.
24. Varalakshmi, V., 2015. A Survey on Secure PIN Authentication for ATM Transactions. International Journal of Advanced Research in Science, Engineering and Technology, II (10), pp. 951-954.