ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Survey of Threats to Automatic Teller Machine (ATM) Payment System in Nigeria

Ugochukwu Onwudebelu
Department of Mathematicsand Computer Science
Federal University of Ndufu, Abaakalik
Ebonyi State, Nigeria
anelectugocy@yahoo.com

Jackson Akpojaro*
Department of Mathematics and Computer Science
Western Delta University
Oghara, Delta State, Nigeria
jakpojaro@yahoo.com

Abstract: The introduction of ATM brought relief to Nigerian banking environment as long queues in the banking hall began to wane; most customers applauded the innovation and opted to transact business through the ATM. However, this relief did not last long as incidences of ATM frauds resulted in decline in customers' confidence. The ATM, a painless access to cash, is now fraught with all kinds of problems and is proving to be a pain in the neck of customers who use it. It has turned out not to be the dream relief it promised as many bank customers have jettisoned their ATM cards and opted to use the old system of cashing money in the banking halls. Like most technology advances, there is always a flaw which criminal-minded individuals identify and exploit to perpetuate fraud. In this paper, we survey and identify sources of threats to ATM victims and their relationships between ATM attackers via the threats and recommendations are made to minimize these threats.

Keywords: ATM fraud, ATM clone, skimmers, closed-circuit television

I. INTRODAUCTION

The impacts of the industrial revolution and globalisation have rapidly increased commercial transactions all over the world. People have realised that exchanging large amount of money was risky; hence people started using banking facilities for different transactions. Although, the automatic debit and credit transactions are now commonplace, the concept of 'invisible' bankers was still relatively new back in the last four decades. The first automated teller machine appeared at a bank in Enfield, North London in 1967. The inventor, John Shepherd-Barron came up with the idea for a cash machine while in the bath. His idea for a cash machine was the first to be tested ahead of other patented devices [1].

The introduction of the ATM technology in 1986 changed the face of banking in Nigeria. It significantly eliminates long queues in banking halls since it offers convenience to customers and provides banking services beyond the traditional brick and mortar service period [2]. The ATM technology caught many Nigerians with surprise for they never thought such delight could emerge in Nigeria because of Nigeria conundrums. Though banks applauded its arrival, however bank customers harboured the fear that the ATM device could turn out to be a veritable avenue for perpetuating fraud. The fear stemmed from the observation that hi-tech cases that involved the ATM have been recorded in more advanced economies of America and Europe [3]. Unfortunately, fears resulting from the problems of the ATM in developing countries could be worse [2]. The challenges facing other businesses in Nigeria – like power outages, telecoms breakdown and others do affect electronic payment platform like ATM services. There are also staff training issues that are to be sorted out, training and re-training of staff displaced by automation and customer/consumer education still lags behind. With regard to power, most ATM machines are run on generators, UPSs and inverters. The once applauded ATM is gradually turning into a problem and targets for theft and vandalism. The seeming transformation experienced in the financial sector has turned sour as many customers do not bother to renew their ATM cards once they expired [4].

II. RELATED WORK

Criminal threats to ATM machines have made headlines in the newspapers [4], [5], [6], [7], [8], and in journals [9], [3]. This is partly because many people from different sphere of life have been negatively affected since the emergence the technology.

The ATM fraud situation in Nigeria is so pathetic that there have been constant stream of research and publications to curb the upsurge. In [10], Azeez et al proposed an expert system which attempts to provide support and help in the investigation of ATM fraud in Nigeria.

Simutis et al [11] proposed a new procedure to supervise ATM network and to detect unexpected behaviour of the ATM system. Launce [12] educated users on how to ensure and carry out safe and secure ATM transactions but failed to expose some emerging threats.

Little [13] describes how grounded theory approach can be used to find factors that influence current and future use of ATM which resulted in the construction of a conceptual model for ATM. McAndrews [14] surveyed literatures which describe the ways ATM systems have influenced aspects of banking markets. Karunanayake et al [2] suggested Mobile-ATM to address the limitations of traditional ATM systems in developing countries. In their proposed solution, people can

withdraw money from a Mobile-ATM without going to a traditional ATM.

We believe that ATM frauds in Nigeria cannot be solved solely by technology because of human factors and lack of infrastructural development. In this paper we investigate the sources of potential threats, relationship between attackers and make recommendations to minimize the threats to ATM facilities in Nigeria.

III. ATM TREATS

There have been many instances of ATM card holders who have been victimized by ATM fraudsters. ATM frauds are often committed mostly by individuals linked to fraudulent bank workers who provide personal identification numbers (PINs) and other relevant information to fraudsters (see Figure 1). Therefore, both banks and ATM customers face problems of ATM frauds. We identify three basic factors responsible for ATM frauds. They are faults of the banks, customers, and criminal activities of ATM fraudsters. These components may appear clear and simple; however they are very complex as there are interplays between these key components. For instance, a fraudulent bank employee who has got the information required to perpetuate ATM fraud may relay such detailed information to an offline or online attacker or decides to be the sole actor, depending on the amount of money and the risk involved.

Sometimes, other cases may be more complex than this. From Figure 1 we can see how these sources of threats interplay between the Bank (dishonest employees), ATM victim (Customer), professional fraudsters (offline attackers and online attackers), and family attacker (customer's family). We think there is a misconception on the part of the customers as to the threats and sources of threats. Most customers believe that they are faced with two threats: the dishonest bankers and fraudsters in particular. But in our survey (see Table 1) we found that there is more to this in terms of dimension. In most cases, customers do not understand the dimension of the fraudsters: offline and online attackers.

Threats from the bank are in three dimensions: lack of closed-circuit television (CCTV), dishonest employees, and database administrators. These three dimensions can be applied by an attacker as in the case of ₦10.5m [9].

Banks and other operators of ATMs have failed to provide certain security measures to protect the customers [8]. For better protection of the customers, banks should install CCTV cameras at every ATM location to strategically monitor who is making transaction. The News magazine survey finds that cameras are not installed at most of the ATM locations in Nigeria [9].

Cases of dishonest bank employees who connived with offline attackers were reported in [6], [5], and [9]. Another bank fraud that could occur at ATMs is when a bank's cash dispensing network is unable to access the database that contains customers' accounts information, especially when database maintenance is being carried out. Though some cases of this nature have been established, however they are not rampant [3].

Customer's faults are of three folds: dishonest customers, customers' carelessness, and family attackers. From experience most customers compromised their PIN/card information with (or without) fraudulent intention. Oni-Orisan [8] identifies the second most common fraud pattern involves theft of ATM cards on which card holders have written out their PINs and carelessly placed them in where they were exposed to other people. Some customers should be held responsible for faults resulting from such acts. Many customers are not discreet enough with their PINs and so, fraudsters take advantage of such carelessness to hack into their accounts and defraud them.

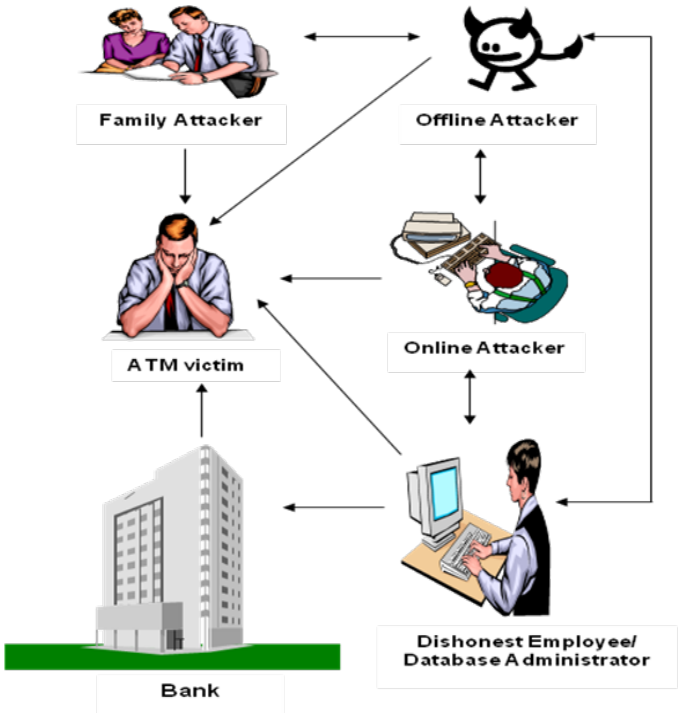

Figure 1: The various Threats that ATM victim faces from Attackers

Our survey reveals that customers' family can be one of the ATM fraudsters (see Table 1). A customer's family includes relatives such as sisters, brothers, friends, and any other person who lives with the customer at home. Some ATM users are just careless with their cards at home, believing that they are safe and never suspect any foul play among the family members. They part with their cards and disclose the front or back of the card to anyone even relatives! It is akin to cash – would you handover your purse or wallet to a stranger? Yet, cases abound where ATM users have been duped by relatives. One in every three ATM frauds involves a member of the cardholder's family [15]. Through pictorial proof provided by CCTV camera, victims have identified close relatives by their appearance and dressing withdrawing cash from their accounts.

Threats from professional fraudsters are in two folds: offline and online attackers. The offline gangs sometimes use skimmers (electronic devices) to store customers' details near crowded ATM machines. In most instances, they are seen punching away numbers in their mobile phones with the information they have got from customers' details. These

details are sent to other gang members who prepare a 'cloned' card with which they withdraw victims' money at ATM machines - this is called 'shoulder surfing'. Some attackers are adapted at spying and quickly memorizing the personal identification numbers of ATM cards at location points and swapping such details on another card through the use of a card reader. Careless use of PINs in ATMs greatly increases the likelihood of PINs being compromised by shoulder-surfing.

The online attackers are determined fraudsters who use the Internet for criminal activities. Some of these online attackers employ some fraudsters to build fake websites of Nigerian banks for them and then use undesirable email to redirect their victims to these fake websites (see Table 1). Some of their email read, "This is to notify you that our services are being upgraded to a new, better and more secured systems. You are now required to CLICK HERE and register all your DEBIT CARDS, X-CHANGE CARDS and CASH CARDS online immediately so as to enable your cards to work on our new services. Only registered cards will work with the new ATM machines. Note that in order to continue using your card for ATM machines, you must register your card(s) online IMMEDIATELY BY CLICKING HERE. If you do not register your ATM cards immediately, you will no longer be able to use your cards with the ATM machines or for ATM transactions and your card will be cancelled or terminated. Adhere to this instruction on receiving this message and CLICK HERE IMMEDIATELY to register your cards. Our goal is to satisfy all our customers need."

These professional fraudsters have a network, the offline and online attackers work together to victimize as many cardholders as possible. They equally work with the family attackers and dishonest bank employees to increase the complexity of their attacks. This is geared at eliminating every trace of futuristic detection and possible apprehension by investigators.

Table 1: Victims of Automatic Theft Machine

S/No	G	Occupation	Defrauded through	Defrauded by	Amount (N)
1	M	Engineer	Email/ATM	Fraudster	800,000
2	F	Media practitioner	ATM	Unknown	40,000
3	M	Businessman	Email/ATM	Fraudster	350,000
4	M	Unknown	ATM	Banker	490,000
5	M	Unknown	ATM	Banker	10.8m
6	F	Unknown	ATM	Unknown	133,000
7	M	Journalist	ATM	Unknown	40,000
8	F	Unknown	ATM	Unknown	45,000
9	M	Businessman	ATM	Unknown	734,000
10	M	Civil Servant	ATM	Unknown	30,000
11	F	Lecturing	ATM	Unknown	120,000
12	F	Unknown	ATM	Family	50,000
13	M	Businessman	ATM	Banker	1.0m
14	M	Journalist	ATM	Banker	25,000
15	M	Student	ATM	Banker	6,000
16	M	System Analyst	ATM	Banker	5,0000
17	F	Businessman	ATM	Fraudster	500,000

* This table is the result from our survey. Many ATM victims revolve around these fraudulent schemes. We choose these few victims to avoid enlarging the table and unnecessary repetitions

IV. DISCUSSION

From Table 1, ATM frauds revolve around bankers, family, and fraudsters using different schemes. Customers are losing lots of money daily, while in most cases the banks are refusing liability, failing to realise the hazardous nature of these happenings. It is the responsibility of the banks to put in place appropriate mechanisms to administer this sophisticated ATM crimes.

Banks always assume that every incidence of unauthorized ATM withdrawal is as a result of customers not protecting their PINs. However, a review of the relevant procedures by the institution that generates and delivers PINs to customers would help in combating ATM frauds. The combination of relevant technology with best practice would effectively minimise ATM crimes.

Many ATM victims have lost so much money because of breach of responsibility and duty of the banks to their customers. A group of ATM victims have come up with a conceivable solution called class action [16]. The essence of this class action is that, rather than instituting an individual claim against banks, ATM victims have come together to institute a single suit as there are common issues, which involve common interests amongst all the parties. A class action suit has been instituted against the CBN, all banks in the country, and other firms before the Federal High Court, Lagos, claiming about ₦50 billion damages [5]. This seems to be the first step of victory for all ATM fraud victims and the Nigerian consumers. We believe this case would be an epoch making and would open up a floodgate of successful litigations against the banks.

As in the U.S. and UK, there is a need for an Electronic Transaction Act (or Code) in Nigeria to protect the rights of customers and banks. The banks have not shown enough duty of care in protecting ATM victims because we have not got any working Act in Nigeria. A victim of an unauthorised ATM withdrawal has a right of action against the bank. There is a duty of care to protect customers' deposits. Between 71% and 81% of ATM fraud cases decided in the U.S. and in the UK were resolved in favour of customers [16]. In Nigeria, we have not got any precedents to guide us as to what the law is. This is yet to be tested, but we believe that the class action case [5] would help establish that, to ascertain whoever that is liable in this case.

It is unfortunate that the country has no system that keeps track of veteran financial fraudsters. Some fraudsters' bankers move from one bank to the other with a view to perpetuating financial crimes. The financial regulatory authority (FRA) needs to mandate banks to conduct a thorough background checks on every potential bank employee [10]. In addition, annual background checks need to be conducted on all existing employees of banks. With access to the convicted financial fraudsters' database, banks can verify if a potential employee has been involved (or convicted) in any form of financial scam in the past. Bankers who have access to the database of customers should also be under the watchful eyes

since customers' accounts can be compromised by fraudulent employees.

Although most banks have started complying with the chip and PIN directive of the financial regulatory body, however, the latest fraud figures from some countries that use the chip and PIN scheme show that financial frauds are still up [17]. The biometric technology which has been applied to validate passport and travel documents, entry into secured areas, and authenticating or securing financial transactions, especially in developed nations should be introduced in conjunction to the chip and PIN [18]. We recommend the following measures to tackle the menace of ATM fraudsters in Nigeria;

a. FRA should pursue the enactment of Electronic Transaction Act (or Code) in Nigeria.
b. FRA should build a national database of convicted financial fraudsters by using modern technology such as biometric, so that personal record of any convicted fraudster can be collected and managed by a clearing house. The benefit is to deter fraudsters from gaining employment at any bank or financial institution in the country.
c. The banks should be able to prove that the customers contributed to the loss of the funds placed in their care by conducting comprehensive investigation on reported ATM frauds.
d. The banks should work together with the Internet Crime Complaint Centre (IC3) in United States to shut down websites that provides cloned service for criminality.
e. The banks should actively cooperate with the Special Fraud Unit (SFU) of the police and Economic and Financial Crime Commission (EFCC) in detecting fraudulent transactions. This will help in reducing incessant cases of ATM frauds.
f. Where there is no CCTV, the ATM owners, the banks, should install CCTV as a priority so as to capture the footage of criminals who exploit the system.
g. Bank employees should be placed under the microscope.
h. Customers should protect their PIN/ Card information from everybody especially family members and friends.

V. CONCLUSION

In this paper we have discussed various sources of threats to ATM operations, and suggested recommendations to address these threats. The health of the financial sector is vital to the growth of the economy. Therefore, the government, financial institutions, and FRA have to be more proactive about the management of the sector by investing in modern technologies and human capital to implement 21st century financial tools in Nigeria. It is inappropriate to use those technologies that have been obsolete in Europe, America and parts of Asia. The use of modern tools would help in minimising ATM fraud in Nigeria as the challenge to curtail fraud in the financial sector is daunting and calls for the collaboration of all stakeholders.

The menace of technology fraud has become part of the negative side effects of technology deployment and increasing tendencies of converging technologies but all stakeholders across the sector have the duty to ensure that such menace is nipped in the bud. These fraudsters are very smart individuals and are always reinventing new strategies and ways to swindle unsuspecting victims.

As an evolving sector, our financial system is moving towards a more secured chip and PIN. The 'chip and PIN' stores data on the chip of the card rather than the magnetic strip of the card. This chip is similar to the chip used for mobile SIM card and is more difficult to 'clone'. This is the standard the entire industry is evolving towards. Certainly, there is no silver bullet method or technology advocated that would guarantee a 100% eradication of ATM frauds. However, the emergence of any new technology to fight a particular financial crime usually minimizes it, even if subverted by criminals [18].

IV. REFERENCES

[1] http://news.bbc.co.uk/, "Inventor of cash machine, John Shepherd-Barron, dies," Last accessed January, 2012

[2] Karunanayake, A., De Zoysa, K., and S. Muftic, "Mobile ATM for Developing Countries," MobiArch'08, ACM, 2008, pp 25-30.

[3] Balogun F., "Automated Problems," *The News Magazine*, vol. 30 No.6, 2010, pp 46-48.

[4] Ishola, Y., "ATM fraud: What safeguard for bank customers?"", http://sunday.dailytrust.com/ (2010). Accessed December, 2011.

[5] Ogbe, P., "Combating the Menace of ATM fraud," http://www.compassnewspaper.com, (2010). Accessed February, 2012.

[6] Ogunseye, T., "N10m ATM fraud lands female banks in court." Sunday Punch, January 10, 2010, pp. 2

[7] Olaleye, B., "Heartaches of ATM," Daily Sun, March 2, 2010, pp45,.

[8] Oni-Orisan, G., "Nigerian ATM Card Holders and Their Bankers," http://www.nigeriavillagesquare.com, Accessed January 2012.

[9] Ayodele F., "Automated Theft Machine: Crooks intensify their fleece of bank account holders through the Automated Teller Machine," *The News Magazine*, vol. 34 No. 3, 2010, pp 39-40.

[10] Azeez N .A., Ajetola A. R., Sulaimon B. A. and Atanda F. A.," Framework from Computer Aided Investigation of ATM Fraud in Nigeria," Pacific Journal of Science and Technology, vol. 11 Issue 1, 2010, pp 356- 361.

[11] Simutis R., Dilionas, D., Bastina, L., "Enhanced Supervision of Automatic Teller Machines via Auto," *associative Neural Networks,*. The 8TH International Conference on Applied Stochastic Models and Data Analysis (ASMDA-2009), 2009, pp. 450-454.

[12] Launce M., "All you need to know to Ensure Safe and Secure ATM Transactions," Africa's Global Bank, www.ubagroup.com, 2009, pp. 1-3.

[13] Little L., "Attitudes towards Technology Use in Public Zones: The Influence of External Factors on ATM use," In Proceeding of CHI '03 extended abstracts on Human factors in Computing Systems, 2003, pp. 990-991.

[14] McAndrews, J., "Automated Teller Machine Network Pricing – A Review of the Literature," Review of Network Economics, vol. 2 No. 2, 2003, pp 146-158.

[15] Kratzer, C., "Protect Your Credit Cards By Las Cruces, NM Guide G-244," Electronic Distribution. Family Resource Management Specialist, 2003.

[16] Kio-Lawson, T., "Nigeria's first Class Action on ATM fraud begins!" http://www.businessdayonline.com, Accessed January 2012.

[17] Murdoch, S, Drimer, S., Anderson, R., Bond, M.,". (2010). Chip and Pin is Broken," IEEE Symposium on Security and Privacy, 2010.

[18] Waturuocha, V., "Use biometrics to tackle ATM fraud," http://www.zenithbank.com/. Accessed January 2012.