Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, August 2010, vol. 15, no.2
(*http://www.arraydev.com/commerce/jibc/*)

Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria – A Case Study of Selected Banks in Minna Metropolis

Adelowo Solomon Adepoju
Lecturer, Department of Computer Science, Federal University of Technology, Minna, Nigeria
Email: **sa.adepoju@yahoo.co.uk**
Adepoju holds B.Tech (Mathematics /Computer Science) and M.Sc (Computer Science). He is presently a PhD student at African University of Science and Technology, Abuja, Nigeria. He is a member of Computer Professional Registration Council of Nigeria (CPN). His areas of interest are Web Programming, Usability evaluation, Human Computer Interaction and Information Technology and Society

Mohammed Enagi Alhassan
Department of Library and Information Technology, Federal University of Technology Minna
Email: **mohammedenagi@yahoo.com**
Alhassan E. Mohammed holds B.Tech in Library and Information Technology. He is presently a studying Information Management and Business Technology at Loughborough University UK His areas of interest are Management Information System and Networking

Abstract

Over time, consumers have come to depend on and trust the Automatic Teller Machine (ATM) to conveniently meet their banking needs. But in recent time there have been a proliferation of ATM frauds in the country even and across the globe. Managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that face financial institutions as fraud techniques have become more advanced with increased occurrences. The ATM is only one of many Electronic Funds Transfer (EFT) devices that are vulnerable to fraud attacks. This paper carried out an empirical research

to analyse the cases of ATM usage and fraud occurrences within some banks in Minna. The research identifies the common ATM fraud, how, where and when these frauds are perpetuated and then proffer security recommendation that should be adhered to by both the banks as financial institutions and the ATM users in order to eliminate or reduce it to the barest minimum.

Keywords: **banking; Automatic Teller Machine (ATM); users**

INTRODUCTION

The traditional and ancient society was devoid of any monetary instruments and the entire exchange of goods and merchandise was managed by the “barter system”. The use of monetary instruments as a unit of exchange replaced the barter system and money in various denominations was used as the sole purchasing power. The modern contemporary era has replaced these traditional monetary instruments from a paper and metal based currency to “plastic money” in the form of credit cards, debit cards, etc. This has resulted in the increasing use of Automated Teller Machine (ATM) all over the world.

The use of ATM is not only safe but is also convenient. This safety and convenience, unfortunately, has an evil side as well that do not originate from the use of plastic money but rather by the misuse of the same.

This evil side is reflected in the form of “ATM frauds” that is a global problem. The use of plastic money is increasing day by day for payment of shopping bills, electricity bills, school fees, phone bills, insurance premium, traveling bills and even petrol bills. The convenience and safety that credit cards carry with its use has been instrumental in increasing both credit card volumes and usage.
The world at large is struggling to increase the convenience and safety on the one hand and to reduce its misuse on the other. An effective remedy for prevention of ATM frauds, however, cannot be provided unless we understand the true nature of the problem.

Brunner et al (2004) states that the ATM fraud is not the sole problem of banks alone. It is a big threat and it requires a coordinated and cooperative action on the part of the bank, customers and the law enforcement machinery. The ATM frauds not only cause financial loss to banks but they also undermine customers' confidence in the use of ATMs. This would deter a greater use of ATM for monetary transactions.

It is therefore in the interest of banks to prevent ATM frauds. There is thus a need to take precautionary and insurance measures that give greater "protection" to the ATMs, particularly those located in less secure areas.

OBJECTIVES OF THE STUDY

The objectives of the study are as follows:

1. To identify various fraud and security threats associated with the use of ATM
2. To evaluate the users opinion on ATM fraud and how offender robs the victim of his/her ATM card, gets the PIN and then uses the card.
3. To know the frequency and occurrence of ATM fraud
4. To know the level of security put in place as regards the use of ATM

ELECTRONIC BANKING

In recent years, banks have made their services increasingly convenient through *electronic banking*. Electronic banking uses computers to carry out transfers of money.

Donell(2003) viewed electronic banking as banking services that consumers can access, by using Network system or an Internet connection to a bank's computer center, in order to perform banking tasks, receive and pay bills, and so forth. Many other financial services can be accessed via the Internet. To most people, electronic banking means 24-hour access to cash through an ATM or paychecks deposited directly into checking or savings accounts (Hillier, 2002).

Diniz(1998) in his view states that Electronic banking encompasses a broad range of established and emerging technologies. Some are ''front end'' products and services that consumers opt for, such as ATM cards and computer banking; others are ''back end'' technologies used by financial institutions, merchants, and other service providers to process transactions, such as electronic check conversion. Some are tied to a consumer bank account; others are unrelated to a bank account but instead store monetary value in a database or directly on a card

AUTOMATED TELLER MACHINE (ATM)

Automated Teller Machine is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip that contains a unique card number and some security information, such as an expiration date. Security is provided by the customer entering a personal identification number (PIN).

According to Steve (2002), ATMs are placed not only near or inside the premises of banks, but also in locations such as shopping centers/malls, airports, grocery stores, petrol/gas stations, restaurants, or any place large numbers of people may gather. These represent two types of ATM installations: on and off premise. On premise ATMs are typically more advanced, multi-function machines that complement an actual bank branch's capabilities and thus more expensive. Off premise machines are deployed by financial institutions and also Independent Sales Organizations (ISOs) where there is usually just a straight need for cash.

Although ATMs were originally developed as just cash dispensers, they have evolved to include many other bank-related functions. In some countries, especially those which benefit from a fully integrated cross-bank ATM network, ATMs include many functions which are not directly related to the management of one's own bank account, such as: Paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees,

taxes, etc.), Printing bank statements, Updating passbooks , Loading monetary value into stored value cards, Purchasing and so on.

Christoslav et al (2003) in a research asserted that ATM services are highly profitable for banks, and banks aggressively market the use of ATM cards. ATMs that are off bank premises are usually more profitable for banks because they attract a higher volume of non-bank customers, who must pay service fees. Unfortunately, customers using off-premise ATMs are more vulnerable to robbery. ATM robberies estimates are derived from periodic surveys of banks conducted by banking associations. According to those surveys, there was an estimated one ATM crime (including robbery) per 3.5 million transactions.

THE ADOPTION OF ELECTRONIC BANKING IN NIGERIA

The ability of Nigerian banks to satisfy and retain their customers in the present post-consolidation era will no doubt depend largely on the development of their Information Technology (IT) infrastructure. In the bid to catch up with global developments and improve the quality of their service delivery, Nigerian banks have invested much on technology, and have widely adopted electronic and telecommunication networks for delivering a wide range of value-added products and services.

They have, in the last few years, transformed from manual to automated systems. Ezeoha (2005) posited that the hype of e-commerce, e-banking and e-everything is gradually being embraced by Nigerian financial institutions who are poised to be in the vanguard of narrowing the digital divide. In its survey on the extent of e-banking adoption by Nigerian banks, the Central Bank of Nigeria (CBN), in September 2002, found out that of the 89 licensed banks in the country, only 17 were offering Internet Banking, 24 were offering basic telephone banking, 7 had ATM (Automated Teller Machines) services while 13 of the banks were offering other forms of e-banking. This implies that as of then, 19.1 percent of the banks were offering Internet banking, signifying that Internet banking was yet to take center stage despite its widely acclaimed benefits against the traditional branch banking practice (Ezeoha, 2005). At present these figures have greatly increased.

Part of the reasons identified by Ezeoha (2005) why Internet banking was having a moderate economic impact in the country includes a lack of adequate operational infrastructure like proper telecommunications and power. In addition, Internet usage in the country has been abused by cyber criminals, thus making its window unattractive for domestic banking operations and legitimate international operations. The inherent fear associated with patronizing Internet Banking services in Nigeria he added, is again reinforced by the growing evidence the world over that dubious Nigerians use fake bank websites to scoop funds from unsuspecting victims, and in some cases using existing bank sites for these crimes.

THE BENEFITS OF ATMS

According to Brain (2000), the benefits that can be derived from ATM usage are so numerous, some are outlined below:

- Flexible account access allows clients to access their accounts at their convenience.

- MFI personnel are not required to be present for transactions and have more time to serve clients.
- Increased hours of operation fit client schedules.
- More clients can be reached beyond the branch network, such as in smaller population centers.
- More low-cost funds are available because ATMs make it easier for clients to deposit savings

Automated teller machine fraud

Emeka (2007) in an article state that as the numbers of ATM card holders continue to grow daily as result of e-payment awareness and deployment of more than 3,000 ATM cash points by Nigerian banks across the country, activities of card fraudsters appear to be on the increase. Majority of Nigerian banks, notably United Bank for Africa, warned ATM card users nationwide against disclosing their ATM card details to a second party as a result of fraudsters who are said to be on the prowl. Diebold (2002) state some ATM Frauds in a paper titled "ATM Fraud and Security". The following Techniques were outlined:

Card Theft: In an effort to obtain actual cards, criminals have used a variety of card trapping devices comprised of slim mechanical devices, often encased in a plastic transparent film, inserted into the card reader throat. Hooks are attached to the probes preventing the card from being returned to the consumer at the end of the transaction.
When the ATM terminal user shows concern due to the captured card, the criminal, usually in close proximity of the ATM, will offer support, suggesting the user enter the PIN again, so that he or she is able to view the entry and remember the PIN. After the consumer leaves the area, believing their card to have been captured by the ATM, the criminal will then use a probe (fishing device) to extract the card. Having viewed the customers PIN and now having the card in hand, the criminal can easily withdraw money from the unsuspecting user's account.

Skimming Devices: Another method of accessing a consumer's account information is to skim the information off of the card. Skimming is the most frequently used method of illegally obtaining card track data. "Skimmers" are devices used by criminals to capture the data stored in the magnetic strip of the card. Reading and deciphering the information on the magnetic stripes of the card can be accomplished through the application of small card readers in close proximity to, or on top of, the actual card reader input slot, so it is able to read and record the information stored on the magnetic track of the card. The device is then removed, allowing the downloading of the recorded data.

PIN Fraud: This can take the following forms:

Shoulder Surfing: Shoulder Surfing is the act of direct observation, watching what number that person taps onto the keypad. The criminal usually positions himself in close but not direct proximity to the ATM to covertly watch as the ATM user enters their PIN. Sometimes miniature video cameras that are easily obtained might be installed discretely on the fascia or somewhere close to the PIN Pad, to record the PIN entry information.

Utilizing a Fake PIN Pad Overlay: A fake PIN pad is placed over the original keypad. This overlay captures the PIN data and stores the information into its memory. The fake PIN pad is then removed, and recorded PINs are downloaded. Fake PIN pads can be almost identical in appearance and size as the original. An additional type of overlay that is more difficult to detect is a 'thin' overlay that is transparent to the consumer. This method used in conjunction with card data theft provides the criminal with the information needed to access an unsuspecting consumer's account.

PIN Interception: After the PIN is entered, the information is captured in electronic format through an electronic data recorder. Capturing the PIN can be done either inside the terminal, or as the PIN is transmitted to the host computer for the online PIN check. In order to capture the PIN internally, the criminal would require access to the communication cable of the PIN pad inside the terminal, which can more easily be done, at off-premise locations.

PATTERNS OF ROBBERY AT AUTOMATED TELLER MACHINES

Michael (2003) identifies some factors which influences fraudsters to rob at ATM points. Understanding the factors that contribute to the problem will help in framing local analysis questions, determine good effectiveness measures, recognize key intervention points, and select appropriate responses. A few studies have provided some data on common ATM robbery patterns. The general conclusions are as follows:

- Most robberies are committed by a lone offender–using some type of weapon–against a lone victim.
- Most occur at night, with the highest risk between midnight and 4 a.m.
- Most involve robbing people of cash after they have made a withdrawal.
- Robberies are somewhat more likely to occur at walk-up ATMs than at drive-through ATMs.

Furst et all (2005) observed that there are several and distinct ATM robbery patterns, each of which presents unique challenges in responding. The most common pattern is for the offender to rob the ATM user immediately after the victim makes a withdrawal. other patterns include the following:

- The offender forces the victim to go to an ATM to withdraw cash
- The offender robs the victim of his or her ATM card, forces the victim to reveal the PIN, and then uses the card
- The offender robs a victim standing at an ATM of other valuables (wallet, watch, jewelry)
- The offender follows someone who has just withdrawn cash from an ATM and robs him or her away from the ATM

AUTOMATED TELLER MACHINE SECURITY

Chris (2006), in his research on Bank ATM Security Advice states that ATM bank cash machines have been incorporated in our way of life. They offer a real convenience to those on the run, but at the same time offer an element of risk. Using a bank ATM machine safely requires awareness and a little planning. Just because a bank ATM

machine is open and available 24-hours a day doesn't mean it is always safe to use it.

He further identifies that Bank ATM robbers are usually males under 25 years of age and most work alone. ATM robbers usually position themselves nearby (50 feet) waiting for a victim to approach and withdraw cash. Half of the ATM robberies occur after the cash withdrawal. Many ATM robbery victims are women and were alone when robbed. Most claim that they never saw the robber coming. Most ATM robbers used a gun or claimed to have a concealed weapon when confronting the victim and demanding their cash.

METHODOLOGY

The research employs a case study of three banks in Minna to find out how frauds are perpetuated with the use of ATM card. The banks are; Intercontinental Bank PLC United Bank of Africa (UBA) and Guaranty Trust Bank (GTB). The population of the study comprise the customers of three banks in Minna, each with 50 ATM users were sampled for study. This gives a total of 150 ATM users.

The research instrument used in this research is structured questionnaire. The questionnaire contains three sections; Section one cater for demographic information of the respondent, section two identifies ATM fraud and section three points out security issues and measures. The questionnaire was a close ended questionnaire to elicit guided responses and for easy analysis.

Data analysis

A total of 83 females (55. %) and 67 males (44.7%) from the three banks participated in the study. The age range is shown in the table below

Table 1: Age range

Age range	Frequency	Percentage (%)
16 – 20	31	20.7
21 - 25	55	36.7
26 – 30	45	30.0
30 and above	19	12.7
Total	150	100

Table 2: Occupation

Occupation	Frequency	Percentage (%)
STUDENT	60	40.0
CIVIL SERVANT	34	22.7
BUSINESS MAN?WOMAN	27	18.0
OTHERS	29	19.3
TOTAL	150	100.0

From table 2 above 40.0% of the respondents are students, 22.7% of the respondents are Civil Servants, 18.0% of the respondents are Business Men/Women and 19.3% of the respondents were categories under others.

Table 3: Causes of ATM fraud

S/N	QUESTION	SD	D	N	A	SA
1	Location of ATM at secluded and high risk areas contribute to fraud and crime perpetuated at ATM	7(4.7%)	28(18.7%)	34(22.7%)	62(4.3%)	19(12.7%)
2	PIN theft and shoulder surfing are common ATM fraud perpetuated by fraudsters	10(6.7%)	26(17.3%)	45(30.0%)	41(27.3%)	28(18.7%)
3	ATMs outside banks are more prone to fraud	21(14%)	19(12.7%)	37(24.7%)	41(27.3(%)	32(21.3%)

SD = Strongly Disagree, A= agree, N=Neutral, A= Agreed, SA=Strongly Agree

Table 4: Incidences of ATM fraud and its Security

S/N	Question	YES	NO
1	Have you ever been a victim of ATM	65 9(43.3%)	85 (56.7%)
2	Are you aware of incidence of ATM fraud	96(64.0%)	54 (36.0%)
3	Do you think the level of security is sufficient	55(36.7%)	95(53.3%)
4	Are you aware of any security guide for the use of ATM	63(42.3%)	87(57%)
5	Is there any means provided by the bank that you can quickly report ATM Fraud incident to the bank	54(36%)	96(64%)
6	ATM fraud is carried out most during the Day	77(51.3%)	73(48%)

DISCUSSION OF RESULTS

From the data gathered in obtaining the most victims of ATM fraud, 41 respondents out of 67 respondents of the male have ever been a victim of ATM fraud. 24 out of 83 respondents of the female have been a victim of ATM fraud. This implies that the males are the major victims of ATM fraud from the study.

Also, 33 out of the 60 respondents of the students have ever been a victim of ATM fraud, 7 out of the 20 respondents of business men/women have been a victim of ATM fraud. The age ranges that are most victims of ATM fraud are respondents of age between 21-25 years.

From the data analysis, 33 respondents out of 55 respondents that are between the ages of 21-25 years have been victims of ATM fraud. This shows that the most victims of ATM fraud are students and ATM users who are not aware of any incidence of ATM

fraud.

Brunner et al. (2004) in their study concluded that the location of ATM is a high determinant to fraud or crime carried out at ATM point. From this research over 75% of the respondents affirm that the location of ATM in secluded place contribute to the fraud perpetuated at ATM point. ATM within the banking premises is more secure than ATMs outside the bank premises Also, it is obvious that the location of ATM in attractive place does not make it prone for fraud.

Diebold (2002) in his view states that the major form of ATM fraud is PIN theft which is carried out by various means; skimming, shoulder surfing, camera, key pad recorder etc. This study elucidates that the common type of fraud perpetuated is PIN theft which is mostly as a result of congestion at ATM points. Other forms of fraud that were enumerated by respondents were; force withdrawal, card theft, and skimming and congestion method fraud at ATM.

Cynthia (2000) states that the 24 hours access to the ATM machine is a double edge sword it has both advantage and disadvantage. It is easy to deduce that ATM fraud is carried out most in the day time. Also there are occurrences at night but most ATM users prefer to make withdraw during the day thus preventing incidences of robbery at night.

On the present level of security provide by banks as regards to ATM. The responses from the tables denote that the security level is poor. Some banks do not provide any means where customers can easily report cases of ATM fraud. ATM manuals or FACTA (Fair and Accurate Credits Transactions Act) is a pertinent document that should be given to ATM users as they are been issued with ATM but from the study this is absolutely neglected. Understanding all these, to implement any security of any level will just be an improvement on the weak security points.

CONCLUSION

The adoption of ATM in Nigeria banks for financial transaction keeps growing and people have realizes the convenience in using ATM. The research shows that customers are much comfortable with the electronic banking system, which ATM is just a segment out of various services of e-banking.

As the usage of ATM is increasing so it openness to security threat is ascending. As the ATM technology is advancing, fraudsters are on drawing board to see how they come up with different fraud skills to beat the security. Various forms of fraud are perpetuated, ranging from; ATM card theft, Skimming, Pin theft, Card reader techniques, PIN pad techniques, force withdrawal and lot more.

Despite this threat, the banks are putting up little effort which is not proportional to rate the fraudsters are working to defraud customers. The technology of ATM keep developing, the fraudsters keep improving ways of crime but the banks are not putting sufficient measures of control to avoid fraud at ATM. The security measures adopted by some banks are obsolete making the measures less significant and allowing fraud at ATM.

References

Brunner, A., Decressin, J. and Kudela, B. (2004): Germany's Three-Pillar Banking System – Cross Country Perspectives in Europe, Occasional Paper, International Monetary Fund, Washington DC.

Chris E. M. (2006). Bank ATM Security Advice: Effective Method of Security Measures.Virtual Banking. Journal of Internet Banking and Commerce, 11(1) (http://www.arraydev.com/commerce/jibc/)

Christolav E. A., Marianne A.H. and Jeanne M. H. (2003). US Consumer's and electronic banking 1995- 2003.Board Division of Consumers and Community Affairs. Los Angeles

Cynthia B. (2000). The measurement of white-collar crime using Uniform Crime Reporting (UCR) Data. S department of Justice, Federal Bureau of Investigation, New York.

Dele, K. (2007). ATM in Nigeria Banking Operation. Nigeria Daily Trust Newspaper, June 12 2007 22

Diebold I. (2002). ATM fraud and security: White Paper, New York.

Donnell Yuks K. (2003), New System of banking; Drawill Publications, New York. 2003, 24-25.

Emeka A. (2007). Fraud Alert - Banks Raise Fresh Alarm on ATMs, Vanguard Newspaper Lagos

Ezeoha, A. E. (2005). Regulating Internet Banking in Nigeria, Problem and Challenges-Part1, Journal of Internet Banking and Commerce 10(3), retrieved from http://www.arraydev.com/commerce/jibc/2005

Ezeoha, A.E (2006), Regulating Internet Banking in Nigeria, Problem and Challenges-Part 2. Journal of Internet Banking and Commerce,11(1) retrieved from http://www.arraydev.com/commerce/jibc/2006

Furst, K, .Lang, W. and Nolle, E. D. (2002) , Internet Banking Development and Prospects: Working Paper, Center for Information Policy Research, Harvard University

Hillier, D. (2002). Money Transmission and the Payments Market, Financial World Publishing, Kent UK.

Michael S.S. (2001).Robbery at ATM: Problem-Oriented Guides for Police Series Problem-Specific uides Series No. 8. New York

Steve W. (2002): Automated Teller Machines; CGAP Staff and Exchange, CGAP IT Innovation Series Los Angeles.