Global Journal of Politics and Law Research
Vol.8, No.4, pp.30-67, July 2020
Published by ECRTD-UK
ISSN: ISSN 2053-6321(Print), ISSN: ISSN 2053-6593(Online)

AN EXAMINATION OF THE LEGAL FRAMEWORK FOR CURBING ATM FRAUD: THE NIGERIAN BANKING INDUSTRY IN PERSPECTIVE

*** Uwem Udok, LL.B (Hons.) (Nig), BL (Lagos), LL.M (Lagos), Ph.D. (Jos) Cert. CLE** (Durban, SA) Associate Professor, Vice Dean and Head of Department of Private Law, Faculty of Law, University of Uyo, Email: uwemudok@yahoo.com, GSM: 08024787818**.**

****Peter Ter Ortese, LL.B (Hons), (Abuja),BL (Hons),LL.M (Calabar) Ph.D Student,** University of Uyo, peterortese@gmail.com, GSM: 08035446931

ABSTRACT: *One of the innovations introduced in the banking industry in Nigeria to fast-track banking processes is the use of Automated Teller Machine (ATM). The deployment of ATM in the banking Industry in Nigeria coupled with the increase in the number of bank customers and branches resulted in the increase in the propensity to commit fraudulent practices through the use of ATM by fraudsters. Fraudsters have devised various means to commit the ATM fraud and swindle customers. Regulatory and institutional mechanisms have been put in place to combat incidences of ATM fraud in the banking industry in Nigeria. This article, therefore, examines these regulatory and institutional mechanisms in the banking industry in Nigeria and make appropriate suggestions for reforms.*

KEYWORDS: legal framework, ATM fraud, Nigerian banking industry

INTRODUCTION

One of the pillars on which the economy of any nation can be erected is the banking industry. It is said to be the grease that lubricates the economic machines of any nation that often prompts regular and at times unjustifiable search light on the performance or non-performance of the industry.[1] The banking industry over the years has developed rapidly in terms of establishment of network of branches, and the number of staff and customers have also increased. There has also been sophistication in the banking services including innovation in the various banking processes designed to fast-track its operations and ensure that banking services are made more accessible to

[1] Akinle O, "Legal and Introductory Framework for the Control and Prevention of Crime in the banking Industry, Ajobola, B and Awa, U. (eds) *Banking and other Financial Malpractices in Nigeria (Lagos and Oxford:* Malthouse Press, (1990) P.1

the customers. One of these innovations is the use of technology which has changed operational processes in the banking industry in Nigeria[2]

One of these technological advancements in the banking industry is the introduction of Automated Teller Machine (ATM).[3] For many bank customers, ATM has made it possible for them to withdraw cash, deposit cash and transfer funds at their convenience without having to perform such transactions through interactions with the bank staff in the banking halls. The introduction of ATM has brought about considerable improvement in efficiency and business processes in the banking sector, but with its attendant negative consequences occasioned by its use in the perpetration of fraudulent activities by fraudsters. Several fraudulent means have been identified as the possible ways or methods of perpetrating ATM frauds in the banking industry in Nigeria and these include but not limited to shoulder surfing, phishing and stolen ATM cards.[4]

There are a number of Nigerian laws and regulations that contain provisions designed to curtail cases of ATM fraud in Nigeria. These fraudsters who brazenly engaged in the perpetration of ATM fraud can be held liable under any of these laws. Sometimes, most cases relating to ATM fraud are cases instituted against the banks by their customers alleging the banks' complicity in the fraud. Since, it is always difficult to establish a case of fraud against the bank, the claimants in such cases often rely on alleged act of negligence on the part of the banks for failing to take necessary measures or steps to prevent the occurrence of such fraud. Some accuse the bank staff of colluding with third parties to perpetrate the fraudulent acts.

This paper will examine the legal framework for curbing ATM fraud and make appropriate recommendations for effective prevention and control of ATM fraud in Nigeria.

Automated Teller Machine

Meaning and Nature of ATM

Automated teller machine (ATM) is an electronic communication device that enables customer of financial institutions to perform financial transactions such as cash withdrawals, deposits, funds

[2] C. Nwaze, "Quality and Internal Control Challenges in Contemporary Nigeria banking" *Zenith Economic Quarterly*, 2008. P.25

[3] The ATM was introduced into Nigerian market in 1989. In Nigeria the first bank to introduce ATM was the Moribund *Societe Generale* (SGBN) in 1990. The trade name for SGBNs ATM was Cash point 24. In 1991, the First Bank Plc came on stream with their own ATM giving it a trade name "First Cash" before the inception of other banks. See "First ATM introduced in Nigeria https://www.protectcle.com>a.as Accessed on 20th May, 2020

[4] C. Nwaze (n.2) P.

transfer and account information inquiries at anytime and without the need for direct interaction with the bank staff.[5]

It is a cash dispenser which is designed to enable customers enjoy banking services without coming into contact with cashiers. ATM combines a computer terminal, record keeping system and cash vault into one unit permitting customers to enter into the bank book keeping system with a plastic card containing a personal identification number (PIN). Once access is gained, it offers several retail banking services to customers. An ATM has also been described as an electronic outlet that allows customers to complete basic transaction without the aid of a branch representative.[6] ATMs are known by a variety of names.[7] Many ATMs have a sign above them indicating the names of the bank or organization that owns the ATM, and possibly including the networks to which it can connect. ATMs that are not operated by a financial institution are known as a white label ATMs.

Introduction of ATM into Banking Industry in Nigeria

In Nigeria, a mechanical cash dispenser, arguable an ATM was introduced in 1986 by the defunct *Societe Generale* Bank. In October, Interswitch ATM system took off.[8] In 1991, First Bank of Nigeria Ltd (then First Bank of Nigeria Plc) introduced its first ATM and it was located at No 35 Marina, Lagos, the headquarters of the bank. It was introduced as part of convenience round the clock.[9] Zenith bank introduced the first ATM Gallery in Nigeria at Plot 276 Ajose Adeogm Street, Victoria Island, Lagos. The Gallery was the first full-fledged bank branch in Nigeria without the human teller in 2007.[10]

It is pertinent to mention that initially ATM in Nigeria was operated as elitist services designed for those desirous of exclusive service. Availability of cards was rare and to obtain the cards, it was a difficult process. Presently, the use of ATM cards has been widely promoted. Banks prefer not to have personal contact with their customers because of the use of ATM cards. In order to compel customers to adopt the use of ATM cards, banks often resort to debiting the account of customers for withdrawing below a certain amount across the counter.[11]

[5] *Automated Teller Machine*. En.m.wikidpedia.org Accessed on 5th May, 2020
[6] Julia Kajan *"Automated Teller Machine* https://www.investopedia.com. Accessed on 14th May, 2020
[7] In USA, it is called Automated Teller Machine (ATM) or sometimes ATM machine. In Canada, it is called Automated Banking Machine (ABM). In British English, it is called Cash Machine and hole in the wall. Others are anytime money, cash time, bank time machine, cash dispenser, cash corner, bank omat etc. ATM (n.6)
[8] "An Assessment of the use of Automated Teller Machine (ATM) in the Banking Industry in Nigeria" https://www.projectclue.com/banking-and-finance/project-topics-mat. Accessed on 8th May, 2020
[9] "First ATM Introduced by First Bank" https://www.firstbanknigeria.com Accessed on 8th May, 2020
[10] "Zenith Bank launches First ATM Gallery" https://allafrica.com Accessed on 8th May, 2020.
[11] Wole Olatokun & Louisa Igbinedion "The Adoption of Automatic Teller Machines in Nigeria: An Application of Theory of Diffusing of Innovation" (2009) 6 *Issues in informing science and Information Technology Journal* 274

In Nigeria, the introduction of ATM by banks and its use by bank customers have gained grounds and the rate of such introduction has increased tremendously in recent times.[12] The increase in the development of ATM by banks and its use by customers became more noticeable especially, after the consolidation of banks. Overtime, both bank customers and banks have found the use of ATM more convenient and faster in bank transactions. Banks charge customers for using ATM. The Central Bank of Nigeria regulates the fees to be charged by the banks for the use of ATM by customers. Apart from the fees charged by banks for the use of ATM by bank customers, banks also charge fees for processing of the debit cards. The debit cards have expiry dates and is usually re-newed after the expiration of the value date.

According to data from the Nigerian Inter-bank Settlement System (NIBSS), the total number of Automated Teller Machine (ATMs) in Nigeria as at 2018 is 18,321. However, the total number of transactions performed is 650.06 million, the transaction value is ₦4.76 trillion.[13]. As at 2017, Nigeria needed an estimated number of 60,000 ATM in order to serve the everyday cash needs of Nigeria while persuading them to keep the bulk of their money in banks. It appears that the number may increase significantly by 2020 in view of the increase in the number of business transactions in the country. However, the development of POS (Point of Sale) in several business outlets may have affected the use of ATM by bank customers since POS to some extent perform the same functions of ATM. During the period of lockdown to check the rising number of Covid 19 cases, many people resorted to the use of POS to carry out their transactions especially buying and selling of goods and payment of services. Business outlets such as supermarkets and filling stations made brisk business using POS.

Types of ATMs

There are two primary types of ATMs. Basic units only allow customers to withdraw cash and receive updated account balances. The more complex machine accepts deposits, facilitate line-of-credit payments and transfer, and access account information. In respect of the more complex machine, the ATM user must have opened an account with the bank that operates the machine. In otherwords, the ATM user must be an account holder with the bank that operates the machine [14]

Basic Parts of ATM[15]

- **Card Reader**
  It reads the chip on the front of the card as well as the magnetic stripe on the back of the card.

[12] *Ibid*
[13] "ATM Cards used in Nigeria"- hppts://naira-metrics.com2019/2020. Accessed on 8th May, 2020
[14] Julia Kagan (n.6)
[15] *Ibid*

- **Keypad**
  This is the part that inputs information including the PIN, the type of transaction and the amount of the transaction
- **Cash Dispenser**
  This part dispenses the cash through a slot in the machine and is connected to a safe at the bottom of the machine where cash is normally loaded by the bank.
- **Printer**
  This is the part that prints the receipt and usually on the request of the customer. The receipt records the type of transaction, the amount and the account balance.
- **Screen**
  The ATM issues prompts that guide the customer through the process of executing the transaction. Information is also transmitted on the screen, such as account information and balance.

Functions of ATM

i. Customers can access their bank deposit or credit accounts in order to make a variety of financial transactions.
ii. Cash withdrawals can also be made through the use of ATM.
iii. Customers can use ATM to check their account balances .
iv. Using an ATM, customers can effect transfer of funds to and from mobile phones.
v. It can also be used to withdraw cash in a foreign country.[16]If the currency being withdrawn from the ATM is different from that in which the bank account is denominated, the money will be converted at the financial institution's exchange rate.
vi. Customers can also use ATM for settlement of bills like DSTV subscription and PHCN bill etc.
vii. ATM can also be used for airtime recharge.
viii. Payment for goods and services can also be carried out through the use of ATM.

ATM Fraud

There is no generally acceptable definition of ATM fraud. It all depends on the manner and form of committing the fraud. However, ATM fraud is the theft of the data stored in a bank card.[17] It is characterized by any unauthorized withdrawals of funds from someone's account from a cash point otherwise known as the ATM machine. In other words, it is an incident whereby money is taken out of an account fraudulently without the consent of the account owner.[18]

[16] Schlicter Serah "using ATM's abroad Travel-Travel Tips- NBC News en.m.wikidpedia.org Accessed on 5-5-2020
[17] A. Abdul "Legal Framework for handling ATM and other Electronic Frauds" Long Essay, University of Lagos, 2010
[18] *Ibid*

Another name for ATM fraud is payment card fraud and it involves the fraudulent use of debit and credit cards. In recent years, there has been proliferation of ATM fraud across the globe.[19] Most banks have not sufficiently educated the customers on the basic usage of cards, resulting in the machine, or panic-stricken customers breaking the glass door to exit the ATM enclosure after a late-night transaction.[20]

The number of ATM fraud has continued to increase due to negligence in the handling of ATM cards by bank customers. Most bank customers compromise their bank account details including their personal identification number to fraudsters. There are also cases where customers give out their PIN number to their driver or relative to withdraw money for them. It means that some cases of ATM fraud are not really due to "fraud" strictly speaking but due to the negligence of the card holder.

Therefore, minimizing losses, mitigating risk and maintaining customer confidence in the ATM channel are logical priorities for banks and others who deploy ATM.[21]. A number of factors predisposed people to being victims of fraud. These include illiteracy, health problems and issues of vulnerability.[22] The problem of Automated Teller Machine (ATM) fraud is global in nature and its consequences on bank patronage should be of concern to the stakeholders in banks. Card jamming, shoulder surfing and stolen ATM cards constitute 65.2% of ATM frauds in Nigeria.[23]

Types of ATM Fraud

Card Skimming

Card skimming remains the number one threat globally. Essentially, skimming refers to the stealing of the electronic card data enabling the criminal to counter-feit the card.[24] It can also be described as devices used by crooks to capture data from the magnetic strips on the back of an ATM card. The skimmer allows the download of personal data belonging to everyone who used it to swipe an ATM. It can capture and retain information from more than 200 ATM cards before being reused. Such personal information includes account numbers, balances and verification

[19] Shubhra Jain "ATM Frauds-Detection & Prevention" (2017) 4 (10) *International Journal of Advances in Electronics*
[20] *Ibid*
[21] *Ibid*
[22] Oludayo Tade, How Nigerian ATM frauds victims are swindled" https://the concersation.com. Accessed on 12th May, 2020
[23] "Automated Teller Machine (ATM) Frauds in Nigeria" https://www.tanfonline.com Accessed on 12th May, 2020
[24] Owen Wild "Six types of ATM attack and Fraud" https://www.ner.com,company/blogs/financial/six-types=of-atm-attacks-and-ffraud. Accessed on 12th May, 2020.

codes associated with each card holder. Consumers experience a normal ATM transaction without noticing the device since it is believed though erroneously, that it is part of the ATM equipment.[25] However, card skimming has been on the decrease, thanks to the deployment of anti-skimming solutions like EMV technology and countless ATM functionality.[26] There are other methods that may be employed to deter card skimming.[27]

Card Trapping

Another name for card trapping is "Lebanese loop" because it comes from its regular use. Trapping is the stealing of the physical card itself through a device fixed to the ATM card.[28] It is a strip of metal or plastic which blocks the ATM card slot causing any inserted card to be retained by the machine allowing it to be retained by the fraudster when the card owner leaves. When a customer walks away, frustrated by not getting the card back, the criminal is able to remove the card and withdraw cash, from the customer's account. To succeed in this kind of ATM fraud, the fraudster needs to know the pin number of the customer. Thus the "droplet" method of stealing a customer's pin is also used by the fraudster in addition to the trapping device. With this method, small drops of oil are placed on PIN pad keys. The drops of oil placed on the pin pad key makes it obvious which keys have been pressed and easy to quickly discern the entered pin.[29]

It is to be noted that not every case of card trapping is caused by a device fixed to the ATM by a fraudster. Card trapping may also be caused by network issues or electrical fault in the ATM. In such a situation, the card automatically ejects on its own and the customer removes it. The card may also be trapped, if at the time of loading cash by the bank officer into ATM, a customer uses the ATM at that particular time.

If the card is trapped in the ATM, the customer should immediately report to the customers service unit of the bank for immediate action to be taken by removing the trapped card and given back to

[25] Shubhra Jain (n.19)
[26] Owen Wild (n.24)
[27] Visual clues such as tape residue near or on a card reader may indicate the former presence of a skimming device. In addition, the following anti-skimming solutions can be introduced:-

- Jittering: Jittering is a process that controls and varies the speed of movement of a card as it's swiped through a card reader making it difficult if not impossible to read card data by the external device.
- Alert Systems: This system monitors routine patterns of withdrawals and notify operators or banks in the event of suspicious activity.
- Chip-based cards: These are the cards house data on microchips instead of magnetic trips. Making data more difficult to produce
- Foreign Object Detection: ATMs that are equipped with this type of technology can alert owners, operators or law enforcement in the event that skimming device is added on the fascia of an ATM. See Shubhra Jain (n.19)

[28] Owem Wild (n.24)
[29] Shubhra Jain (n.19)

the customer. The bank will have to confirm that the customer is that true owner of the card before handing over to the customer.

Website Spoofing

This is the act of creating a website as a hoax with the intention of misleading readers that the website has been created by a different person. This is usually done with a fraudulent intention of getting information as to the card details of a user.[30]

Phishing

Phishing operates by sending forged e-mail, impersonating online auction or payment site. The e-mail purport to be official bank request. They ask customers to confirm their online banking details either by e-mail or by entering them into a website. The information thus stolen is used to perpetrate all sort of fraud.[31]

In Nigeria, it is not uncommon to receive massages in GSM phone or personal calls from fraudsters popularly called yahoo boys purporting to be bank staff requesting for customers account details like BVN numbers, account numbers, PIN numbers, and ATM numbers for the purpose of updating them for the customers. If unsuspecting customer of the bank compromises his/her account details, the information is used by the fraudster to carry out unauthorized withdrawals from the account of the customer.

Shoulder Surfing

This is unauthorized or illegal direct observation by a fraudster when an ATM user taps an ATM pin pad. The fraudster stands closely behind the ATM user looking over the ATM user's shoulder to get information especially the pin code. Sometimes, the fraudster may not stand in direct proximity to the ATM user but may position himself close to the ATM user and watch covertly as the ATM customer enters his or her pin.[32]. Another method of shoulder surfing is where the fraudster smartly under the pretext of offering assistance to customers but exchange their non-workable ATM cards to the genuine customer's own. The fraudster would pick the real ATM cards and also spy on the pin code of the genuine customers' cards.[33]

Stealing PIN

[30] Ajayi Abdul (n.17)
[31] Uwem Udok "An Examination of the E-Banking Fraud: The Nigerian Banking Industry in Perspective" (2009) 1(1) *Confluence Journal of Private and Property Law,* 51
[32] Shubhra Jain (n.19) 82
[33] "Police arrest ATM Fraud Syndicate, recover 30 ATM cards I Enugu" https://guardian.ng/news/police-arrest-atm-fraud-syndicate-recover-30-atm-cards-in-enugu- Accessed on 13th May, 2020

Customers often compromise their account details including their Personal Information Number (PIN) to fraudsters. Once the fraudster is in possession of the ATM card of the customer and has knowledge of the PIN through any of these methods like shoulder surfing, skimming device, fake PIN pad overlay[34] and pin interception,[35] the fraudster can withdraw from the account of the customer using the ATM card and the stolen PIN.

Physical Attacks

This category is related to any attempt to rob the ATM of the cash in the safe. Methods of physical attacks include solid and gas explosive, as well as removing the ATM from the site and then using other methods to gain access to the safe.[36]

ATM located in an open place, shopping malls, filling stations, educational institutions and market areas are prone to physical attacks by armed robbers since in most cases security personnel are not available at the ATM terminal to guard the facility. However, ATM located inside the banking halls or within the premises of the bank is more secured than the one located outside the bank premises because of presence security personnel in and around the premises of the bank.

Logical Attacks

In this type of attack, external electronic devices or malicious software is used in the crime. The tools are used to allow the criminal or fraudster to take physical control of the ATM dispenser to withdraw money, which is often called "Cash out" or "Jackpotting" as the machine starts spitting out bills like a casino gaming machine.[37]

Cash trapping

In this type of ATM fraud, the fraudster will use a device to physically trap the cash that is dispensed and come to collet once the customer has left the ATM location. A customer who will withdraw the amount will not notice the device and when he tries to get the money withdrawn, he will have a hard time since the cash will be trapped inside. As soon as the disappointed customer leaves the ATM to ask for assistance, the fraudster who is hanging around the ATM to observe what happens, will quickly remove the device including the cash still glued on it.

[34] A fake PIN pad is placed over the original keyboard. This overlay captures the PIN data and stored the information into the memory. The fake PIN pad is then removed and recorded PINS are downloaded.
[35] After the PIN is entered by the customer, the information is captured in electronic format through an electronic data recover. Capturing the PIN can be done either inside the terminal or as the PIN is transmitted to the host computer for the outline PIN check. In order to capture the PIN internally, the fraudster would require access to the communication cable of the PIN pad inside the terminal which can easily be done at off premises locations.
[36] Owem Wild (n.24)
[37] *Ibid*

There are variety of ways used by fraudsters to trap cash in the ATM. These are by installation of a fabricated ruler device, a false ATM presenter and transaction Reversal.[38]

i. A fabricated ruler device

As already stated, the fraudster uses a device that looks like a ruler to trap cash in ATM.

ii. A false ATM Presenter

This fraud is performed through the addition of bill traps or false presenters in front of ATM dispensers. These traps are placed over to disguise the normal dispensing operation of the ATM. During normal dispensing transaction, an ATM will dispense notes into the trap but those notes are never presented to the customer. The customer will leave thinking that the ATM is faulty only for the fraudster to return to the ATM and remove the bill trap or false presenter, and leaves with the cash that was intended for the customer. To guard against ATM fraud through a false ATM presenter, the presenter door mechanics can be enhanced with a more robust locking mechanism.[39]

Transaction Reversal

This is sometimes called "dispensing error" but most dispensing errors are not fraud related; it may be due to network issues. Transaction reversal scams use variety of methods to create an error condition at the ATM, which result in a transaction by the host processor due to the reported inability to dispense cash, while the cash is legitimately accessible.[40]

It is pertinent to state that where the dispensing error is not a scam and the customer is debited, the transaction will reverse and the customer's account is credited. Banks often advise customers to wait for 24 hours for the reversal to be affected and if after the expiration of 24 hours, the transaction does not reverse, the customer is given a form to fill stating the amount involved, the date of transaction, the bank ATM and the time of dispensing error. Sometimes, it may take several days or weeks or even months (in rare cases) for the bank to credit the account of the customer. In some cases, where the process drags for a longer period of time, the customer becomes frustrated and abandon the process. Later, the customer's account is either credited by the bank or if not credited, the bank may allege that the transaction was successful and so the customer is deemed to have successfully withdrawn the money from the ATM. The option available to the customer is to sue the bank for the refund of the debited amount. In the case of *Elder Ekong Akpan Udofia v First Bank of Nigeria Ltd*.[41] the Plaintiff by a Writ of Summons dated 22/6/2016 and filed the same date, claimed against the defendant, *inter-alia* as follows:

[38] Shubhra Jain (n.19)
[39] *Ibid*
[40] *Ibid* 85
[41] Suit No HEK/46/2016 (unreported) Judgment delivered by Justice Nsemeke Daniel of the Eket High Court, Eket, Akwa Ibom State on 5th April, 2017

i. An order of court declaring the act of the Defendant's neglect, failure and refusal to credit the account of the Plaintiff with the sum of ₦180,000 (One hundred and eighty thousand naira) which said amount is out-standing as unpaid sum from the amount which was wrongly debited on his account by the Defendant over failed ATM transaction as an act of negligence, thus unlawful.
ii. An order of court directing the Defendant to credit the account of the Defendant at its Eket branch with the sum of ₦180,000 (one hundred and eighty thousand naira) which said amount is out-standing as unpaid sum from the amount which was wrongly debited on the Plaintiff's account by the Defendant over failed ATM transactions and ₦455.00 (Four hundred and fifty five Naira) charged on ₦65.00 for seven times in respect of the failed transactions together with interest as appropriate.

In the Statement of Claim, the Plaintiff averred that he carried out transaction on 4/3/15 with his ATM Card at Diamond Bank ATM machine for ₦80,000, he was debited but he was not paid, cash. Furthermore, on the 7/4/15, he carried out another transaction with his card at Ecobank ATM for ₦80,000. Again, he was debited but he was not given cash. Furthermore, on 9/5/15 he attempted to withdraw N40,000 at the Defendant's ATM. His account was again debited but cash not dispensed to him. Lastly, on 13th April, 2015, he tried to withdraw ₦60,000 at the FCMB ATM, his account was debited but cash not dispensed to him. In all these failed transactions, he claimed that the defendant charged him ₦65.00. However, he averred that only ₦80,000 was refunded to him after much pressure.

The Defendant in it's defence averred that all alleged failed transactions except the case of the ₦80,000 refunded to the Plaintiff were reversed and successfully paid to the Plaintiff. In support of its claim, the Defendant tendered Exhibit D4, Journal Paper showing the entire transactions on each of those days indicating that there were no dispense errors and the withdrawals were successful except that of the ₦80,000.
The court held that the Plaintiff proved his claim for the failed transactions of 9/4/2015 and 13/4/15 in the sum of ₦40,000 and ₦60,000 respectively and ordered for a refund of the entire sum of ₦100,000 as well as the charges deducted from the Plaintiff's account as a result of the failed transactions amounting to ₦455.00.

Legal Regimes for Curbing ATM Fraud

Since the introduction of electronic banking in Nigeria, the government and the relevant regulatory agencies have striven to match the rapidly changing electronic banking environment with

necessary regulations and institutional framework. Efforts have been made in the area of enactment of relevant legislations to regulate electronic banking in Nigeria.[42]

With the introduction of electronic banking in Nigeria, the increase in the number of customers using electronic banking to transact business increased the propensity perpetrate electronic fraud including ATM fraud. This necessited strict regulatory measures to deal with these fraudulent practices. There are existing laws and regulations that either directing or indirectly help in curtailing cases of ATM fraud in Nigeria.

Central Bank Guidelines on Electronic Banking In Nigeria

Consequent upon the introduction of Electronic banking in Nigeria, the CBN recognized that electronic banking and payments services are still at the early stages of development in Nigeria. Arising from the three major roles of the CBN in the areas of monetary policy, financial system stability and payments system oversight, the CBN technical committee on E-Banking produced a report which anticipated the likely impact of the movement towards electronic banking and payment on the achievement of CBN's core objectives.

Following from the findings and recommendations of the committee, four categories of guidelines were developed as follows:[43]

i. Information and Communication Technology (ICT) Standards, to address issues related to technology solutions deployed and ensure that they meet the needs of consumers, the economy and international best practice in the areas of communications, hardware, software and security.
ii. Monetary policy, to address issues relating to how increased usage of interest banking and electronic payment delivery channels would affect the achievement of Central Bank of Nigeria Monetary Policy objectives.
iii. Legal guidelines to address issues on banking regulations and consumer rights protection.
iv. Regulatory and supervisory, to address issues that though peculiar to payment system in general may be implied by the use of electronic media

Despite numerous key provisions of the Guidelines, few sections deal with issues relating to ATM. Banks are encouraged to put in place procedures for maintaining the banks website, including the various security features needed for electronic banking services

The Guidelines

1. Technology and Security Standards

[42] Failed Banks (Recovery of Debts) and Malpractices in Banks Act Cap F2 LFN 2004; Money Laundering (Prohibition) Act 2011. Advance Fee and Other Fraud Related Offences Act, 2006

[43] Preamble, Central Bank of Nigeria, Guidelines on Electronic Banking in Nigeria, August, 2003. P.I

CBN will monitor the technology acquisitions of banks, and all investments in technology, which exceed 10% of the funds will henceforth be subject to approval. Where banks use third parties or outsource technology, banks are required to comply with the CBN guidelines.

2. **Automated Teller Machines (ATM):** in addition to guidelines on e-banking in general, the following specific guidelines apply to ATMS:
   a. Networks used for transmission of ATM transactions must be demonstrated to meet the guidelines specified for data confidentiality and integrity.
   b. In view of the demonstrated weakness in the magnetic stripe technology, banks should adopt the chip (smart card) technology as the standard, within 5 years. For banks that have not deployed ATMs, the expectation is that chip based ATMs would be deployed. However, in view of the fact that most countries are still in the magnetic stripe conversion process, banks may deploy hybrid (both chip and magnetic stripe) card readers to enable the international cards that are still primarily magnetic stripe to be used on the ATMs
   c. Banks will be considered liable for fraud arising from card skimming and counterfeiting except where it is proven that the merchant is negligent. However, the cardholder will be liable for frauds arising from PIN misuse.
   d. Banks are encouraged to join shared ATM networks.
   e. Banks are required to display clearly on the ATM machines, the acceptance mark of the cards usable on the machine.
   f. All ATMs not located within bank premises must be located in a manner to ensure the safety of the customer using the ATM. Appropriate lighting must be available at all times and a mirror may be placed around the ATM to enable the individual using the ATM to determine the locations of persons in their immediate vicinity.
   g. ATMs must be situated in such a manner that passersby cannot see the key entry of the individual at the ATM directly or using the security devices.
   h. ATMs may not be placed outside building unless such ATM is bolted to the floor and surrounded by structures to prevent removal.
   i. Additional precaution must be taken to ensure that any network connectivity from the ATM to the bank or switch are protected to prevent the connection of other devices to the network point.
   j. Non-bank institutions may own ATMs, however such institutions must enter into an agreement with a bank or the processing of all the transactions at the ATM. If an ATM is owned by a non-bank institution, processing banks must ensure that the card readers, as well as, other devices that captures/stored information on the ATM do not expose information such as PIN number or other information that is classified as confidential. The funding (cash in the ATM) and operation of the ATM should be sole responsibility of the bank.

k. Where the owner of the ATM is a financial institution, such owner of the ATM must also ensure that the card reader as well as other devices that capture information on the ATM does not expose/store information such as the PIN number or other information that is classified as confidential of the ATM.
l. ATMs at bank branches should be situated in such a manner as to permit access at reasonable time. Access to the ATMs should be controlled and secured so that customers can safely use them within the hours of operations. Deployers are to take adequate security steps according to each situation subject to adequate observance of standard securities policies.
m. Banks are encouraged to install cameras at ATM locations however, such cameras should not be able to record the keystrokes of such customers
n. At the minimum, a telephone line should be dedicated for fault reporting, such a number shall not be dedicated for fault reporting, and such a number shall be made known to users to report any incident at the ATM. Such facility must be manned at all times the ATM is operational.

A careful examination of some of the above guidelines in relation to ATM is necessary. With reference to deployment of ATM with magnetic stripe, most banks have complied with this guideline. The danger associated with the deployment of magnetic stripe based ATM is that it is susceptible to fraudulent manipulation though skimming. Banks should ensure that anti-skimming device is installed in the ATM, otherwise, where allegation of ATM fraud is as a result of card skimming, the bank may not escape liability where there is no anti-skimming device installed by the bank in the ATM. On liability of the card holder for fraud arising from PIN use, any customer who compromises his credentials to third parties cannot hold the bank liable for fraud or negligence. In *Benjamin Agi v Access Bank Plc. Ogbuinya, JC.A* stated as follows:[44]

> "I am impelled to draw that inference that it was either the appellant that did the withdrawal or an unknown third party to whom he divulged the PIN… were it to be otherwise the respondent would have been held responsible for that withdrawal- a flagrant breach of its duty to shield the appellant's funds from scrupulous third parties".

On the issue of location of ATM, the guidelines enjoin banks to ensure that all ATMs not located within the bank premises must be located in a manner to ensure the safety of the customer using the ATM. It is submitted that ATM should not be located at a corner of a building, as corners create

[44] (2014) 9 NWLR (P14111)192

a blind area. An ATM further from a corner, preferably near the center of the building reduces the element of surprise by an assailant and increase effective reaction time by the user.[45]

Most banks do not have video surveillance like closed circuit Television cameras mounted on the premises where the ATM is located outside the premises of the bank. In most locations where ATMs are located outside the premises of the bank, there are no perimeter fences and numerous entry and exit points can be found. These are potentials avenues for fraudsters to take advantage to perpetrate their criminal acts.

The guidelines allow non-bank institutions to own ATMs, this is a laudable provision, but in most cases, ATM frauds are committed in the premises of these non-bank institutions because those places are vulnerable to criminal activities, especially those located in educational institutions, market areas, shopping malls and filing stations. The ATMs are often exposed to physical attacks including solid and gas explosives as well as removing the ATM from the site and then using other methods to gain access to the safe by criminals.

The guidelines provide for telephone lines to be dedicated by the bank for fault reporting. Unfortunately, most banks do not provide any dedicated telephone line for fault reporting. Most customers are often helpless when their cards are trapped inside the ATM or they experience dispensing error and there is no means to communicate to the bank to seek solution. The situation becomes worst during weekends and Sundays.

Central Bank of Nigeria Standards And Guidelines on Automated Teller Machine (ATM Operation in Nigeria

Preamble

Pursuant to section 28(b) of the Central Bank of Nigeria Act,[46] the Central Bank of Nigeria (CBN) is authorized to issue guidelines, rules and standards for the maintenance and reasonable financial services for the public and to ensure good conduct and management of the financial system.

The primary purpose of issuing the guidelines is to ensure the efficiency of ATM service and convenience as well as protection of customers institutions, viz, banks, non-banks or acquirer deploying ATMs or any card issuing outlet issuing card for ATM use shall comply with the standards and guidelines with respect to each of the ATM facilities within its dominion and control. The standards and guidelines are stated hereunder

[45] Shubhra Jain (n.19)
[46] *Ibid*

The Standards

1. Standards on ATM Technology and Specification:

a. All ATM deployers/acquirers shall comply with payment Card Industry Data Security Standards (PCIDSS).
b. All ATMs shall be able to dispense all denominations of Naira.
c. All terminals shall be levels 1&2 EMV complaint and shall be upgraded from time to time to comply with the latest version within six months of release of the version.
d. All ATMs shall have audit trail and logs capabilities, comprehensive enough to facilitate investigations, reconciliation and dispute resolution.
e. Card readers shall be identified a symbol that:
    i. Represent the card;
    ii. Identifies the direction for which the card should be inserted into the reader
f. 2% of ATMs deployed shall tactile graphic symbol for the use of visually impaired customers. This should be complied within five years from the release of these standards.
g. All new ATMs shall accept card horizontally with the chip upwards and to the right.

2. The Guidelines

ATM deployment

a. All ATM consortia may own ATMs; however, such institutions must enter into an agreement with a card scheme or a scheme operator or their designated settlement agent for acceptance and settlement of all the transactions at the ATM.
b. Banks shall only deploy ATMs within their premises while the deployment of ATMs outside bank's premises should be left to CBN approved consortia provided that no card scheme or any company that a card scheme has shareholding or ownership of more than 20% will be licensed as ATM owner or acquirer.
c. All ATM transactions in Nigeria shall be processed by a Nigerian company operating in Nigeria as acquirer-processor.
d. No card or payment scheme or Card Association shall compel any issuer or acquirer to send any transaction outside Nigeria for purpose of processing, authorization or switching if the transaction is at an ATM or any acceptance device in Nigeria and the issuer is a Nigerian bank or any other issuer licensed by the CBN.
e. All transactions at an ATM in Nigeria shall, where the issuer is a Nigerian bank or any other issuer licensed by the CBN settled under a domestic settlement arrangement operated by a Nigerian Company. All collaterals for such transactions shall be in Nigerian National Currency and deposited in Nigeria.

f. No card scheme shall discriminate against any ATM owner or acquirer. Every card-scheme must publish for the benefit of every ATM owner or acquirer and the Central Bank of Nigeria the requirement for acquiring ATM transaction under the card scheme.
g. No ATM owner or acquirer shall discriminate against any card scheme or issuer.
h. Stand-alone or closed ATMs are not allowed.
i. ATMs should be situated in such a manner as to permit access at reasonable times. Access to these ATMs should be controlled and secured so that customers can safely use them.
j. Lighting should be adequate for safe access and good visibility. It should provide a consistent distribution and level of illumination, particularly in the absence of natural light.
k. ATMs should be sited in such a way that direct or reflect sunlight or other bright lighting is prevented from striking the ATM display, for example, through the use of overhead sun shelter.
l. Privacy shall be provided by the design and installation features of the ATM so that in normal use of cardholder does not have to conspicuously take any protection action.

ATM Operations:

A bank is an independent organization that deploys an ATM for the use of the public and shall ensure that:

a. The ATM downtime (due to technical fault) is not more than seventy-two (72) hours consecutively;
b. The helpdesk contacts are adequately displayed at the ATM terminals. At the minimum, a telephone line should be dedicated for fault reporting and such telephone facility shall be functional and manned at all times that the ATM is operational.
c. All ATM surcharges are fully disclosed to customers;
d. The ATM issue receipts, where requested by a customer, for all transactions except for balance enquiry, stating a minimum the amount withdrawn, the surcharges, date and time of the transaction;
e. Receipt prints and screen display are legible.
f. The dispensing deposit and recycling of the machine is in proper working condition;
g. The dispensing component holds out notes of the collection of the user for a minimum of twenty (20) seconds;
h. There is appropriate monitoring mechanism to determine failure to dispense cash;
i. There is online monitoring mechanism to determine ATM vault cash levels
j. ATM vault replenishment is carried out often as possible to avoid cash-out.
k. ATMs are not stocked with unfit notes;
l. Availability of cash in the ATMs at all times. The funding and operation of the ATM deployed by non-bank institutions should be the sole responsibility of the bank or institutions that entered

into agreement with them for cash provisioning. In this regard, the Service Level Agreement (SLA) should specify the responsibilities of each of the parties.

m. Change of PIN provided to customers free of charge throughout the entire value chain.
n. Acquirers monitor suspicious transactions and report statistics to CBN based on the agreed format and timeframe.
o. Back-up power (inverter) is made available at all ATM locations in such a way that the machine would not cease operation while in the middle of a transaction.
p. Waste disposal basket is provided at all ATM locations.
q. A register of all their ATMs in Nigeria with location, identification, serial number of the machines, etc is maintained.
r. Provision is made for extending the time needed to perform a specific step by presenting a question, such as, "Do you need more time?"
s. Information sufficient to construct a usable card is not displayed on the screen or printed on a transaction record. This will guard against the possibility that such information may become accessible to another person should the cardholder leave the ATM while a transaction is delayed, or abandon a printed transaction record.
t. Precautions are taken to minimize the possibility of a card being left by a massage or voice alerting the customer to take his card.
u. Cash out first before card is out of the ATM is adopted to minimize the possibility of customers leaving cash uncollected at ATM.
v. ATM acquirers that disable cash-retract shall display such notice at the ATM or on the screen.
w. Every ATM Consortium or acquirer of ATM or POS shall drive its ATMs or POS directly and shall not outsource the driving of its ATMs or POS to any Card Scheme or Switch and all transactions from the ATM or POS shall first go to the ATM Consortium or acquirer.

ATM Maintenance

A bank or independent organization that deploys an ATM for the use of the public shall ensure that:

a. Notice is displayed at the ATM for planned maintenance period and disruption to service due to maintenance for public;
b. An ATM maintenance register or log is kept properly
c. All ATM and cash in the machines are insured.
d. They physically inspect their ATMs at least fortnightly.

ATM Security

i. Every ATM shall have cameras which shall view and record all persons using the machines and every activity at the ATM including but not limited to: card insertion, PIN entry, transaction selection, cash withdrawal, card taking, etc. however, such cameras should not be able to record the key strokes of customers using the ATM.
ii. Where a surveillance camera is used, it should be kept secretly to avoid thieves removing or damaging or compromising it.
iii. Networks used for transmission of ATM transactions must be demonstrated to have data confidentiality of their integrity.
iv. All ATMs must be located in such a manner that guarantees safety and security of users and confidentiality of their transactions.
v. ATM should not be placed outside building unless such ATM is bolted to the floor and surrounded by structures to prevent removal.
vi. Additional precaution must be taken to ensure that any network connectivity from the ATM to the bank or switch is protected to prevent the connection of other devices to the network point.
vii. Where the user of an ATM blocks his image for camera capture, the ATM shall be capable of aborting the transaction.

Dispute Resolution

In the event of irregularities in the account of an ATM customer arising from the use of card on ATM, the following shall apply:

a. All cardholders' complaints should be treated within a maximum of 72 hours from the date of receipt of the complaints.

Penalties

Sanctions, in the form of monetary penalties or suspension of the acquiring/processing service(s) or both, would be imposed on erring institutions for failure to comply with any of the provisions of the ATM standards and guidelines or any other relevant guidelines issued by the CBN from time to time.

A critical examination of some of the above standards and guidelines of ATM operation is necessary. Paragraph 3.2 of the Guidelines provides for ATM operations by bank and independent organizations. It makes it mandatory for adequate display of helpdesk contacts at the ATM terminals at the minimum, a telephone line should be dedicated for fault reporting and such telephone facility shall be functional and manned at all times that the ATM is operational. Most of the ATM terminals, if not all do not have helpdesk contacts as provided in the guidelines. The helpdesk contacts are supposed to have functional telephone lines that customers can call to request for assistance or lodge complaints when they face challenges associated with the use of the ATM. For instance, dispense error, card or cash trapping or network issues or outright fraud.

The Guidelines provide for all ATM surcharges to be fully disclosed to customers.[47] Early this year, CBN released the new charges to be deducted by banks as ATM charges.[48] Banks in most cases do not comply with the new CBN charges and their charges are different from the ones approved by the CBN. The banks have now devised a means of deducting ATM charges without sending the alert to their customers. This is fraudulent and in violation of paragraphs 3.2 (c) of the Guidelines which states that all surcharges should be disclosed to customers. It should also be noted that pursuant to the revised guide to bank charges, banks are not expected to charge customers on ATM card maintenance in respect of current account but can charge maintenance fee on savings account.[49] Banks also charge customers for processing of ATM cards as well as renewal of such cards upon expiry.

On the issue of receipt, some banks' ATMs do not print receipts upon request by the customer because either the printing device is faulty or there is no paper in the ATM to print the receipt. The customer is therefore kept in dark as to transactions he has carried out in the ATM since there is no receipt evidencing the transactions.

On change of PIN, the Guidelines provide that change of PIN is provided to customers free of charge. The issue is not on the change of PIN to customers free of charge but who facilitates the PIN change. A situation where a private security personnel attached to the bank is directed by the bank officer to accompany the customer to the ATM terminal to assist the customer to change the PIN is improper. The security officer may take advantage of an illiterate or sick customer to steal the PIN number and perpetrate fraud. Banks must show their customers how their cards work and how to get help when in trouble. Security officers who are not bank staff should not be allowed to deal with customers.[50]

[47] Paragraph 3.2 (c)

[48] The Revised Guide to bank charges released by the CBN contain the new charges for ATM deduction by banks. The Revised Guide to Bank charges took effect from January, 01, 2020. Based on the CBN directive banks and non-financial institutions were mandated to reduce charges applicable to bank accounts electronic transfers, and Automated Teller Machine (ATMs). For ATM withdrawals, charges after 3rd withdrawals on another bank's ATM in the same month is now ₦35.00 as against the old charge of ₦65.00. For card maintenance in respect of savings account, it is now ₦50.00 quarterly as against the old charge of ₦50.00 monthly. For current account, there is no charge as against the old charge of N50.00 monthly. See A. Ojekunle "Nigerian Banks begin implementing of new charges on ATM, e-Transfer" https//www.pulsse.ng/bifinancenigerian-banks-beginomplementing-ofnew-charges-on-atm-e-transafer/ijigzrm- Accessed on 18/5/2020.

[49] *Ibid*

[50] Oludayo Tade "How Nigerian ATM fraud victims are swindled" https://the conversation.com/how-nigerian-atm-fraud-victim-are-swindled-8774, accessed on 12-5-2020

Paragraph 3.4 of the guidelines provide for ATM security. Specifically, it makes it mandatory for every ATM to have cameras which shall view and record all persons using the machines and every activity at the ATM. This is a laudable provision and it is also contained in the CBN Guidelines on Electronic banking in Nigeria. Such cameras will capture the image of any fraudster who perpetrates fraud using the ATM. The issue of non-installation of camera came up in the case of ***Ekong Archibong v First Bank of Nigeria Plc***,[51] the Plaintiff claimed that the Defendant did not implement the CBN guidelines on security devices in relation to ATM transaction. This fact was not pleaded in the Statement of Claim and the Plaintiff raised it during cross-examination. The court held *inter-alia* that evidence led or brought to the fore outside pleadings go to no issue more particularly unpleaded evidence elicited during cross examination is admissible. Consequently, that unpleaded evidence was expunged from the record of the court.

Paragraph 2.5 of the Guidelines deals on Dispute Resolution. It makes it mandatory for all cardholder's complaints should be treated within a maximum of 72 hours from the date of receipt of the complaints. Unfortunately, such complaints lodged by customers in respect of irregularities in their account arising from the use of ATM often take longer periods up to one or two months before such complaints are treated by the banks. Recently, the CBN revised the timeframes for the resolutions of all botched online transfers, Pos. transactions and ATM withdrawals. Pursuant to this revision, Nigerian banks are required to reverse instantly, any failed ATM transaction that occurs when a customer tries to withdraw from the bank. However, in the event that the instant reversal fails due to technical challenges, the money must be manually reversed within a 24-hour period. This revision will take effect from 8th June, 2020.[52] Prior to this new directive by CBN, the timeframe for such reversal is usually three working days. Therefore, it is necessary to update the CBN Guidelines on ATM operations in line with this new directive.

On the issue of penalties,[53] the Guidelines do not make specific mention of the monetary penalty(ies) to be imposed on erring banks in the event of non-compliance. It makes a blanket imposition of monetary penalties or suspension of the acquiring/processing service or both. There is need for specification of the monetary penalties to be imposed on erring banks

Advance Fee Fraud and Other Fraud Related Offences Act.

[51] HU/355/2010 Judgment delivered by Justice Ifiok Ukana (Retired)
[52] Emmanuel Benson, "CBN revises timeline for resolution of dispense error, refunds complaints" https://nairametrics.com. Accessed on 5th June, 2020.
[53] Paragraph 5.0

The Advance Fee Fraud and other Fraud Related Offences Act was enacted in 1995.[54] It was later amended the same year.[55] In 2006, the Advance Fee Fraud and Other Fraud Related Offences Act was enacted.[56]

The felony of obtaining property by false pretense is committed where a person by any false pretence and with intent to defraud obtains from any other person anything capable of being stolen or induces any other person to deliver to any person capable of being stolen.[57] Obtaining by false pretence means knowingly obtaining another person property by means of a misrepresentation of fact with intent to defraud. Section 1(1) of the Act[58] provides as follows:

Notwithstanding anything contained in any other enactment or law, any person who by any pretence had with intent to defraud.

a. Obtains from any other person, in Nigeria or in any other country for himself or any other person,
b. Induces any other person in Nigeria; or
c. Obtains any property whether or not the property is obtained or its delivery is induced through the medium of a contract induced by the false pretence is guilty of an offence under this Act.

Section 1(1) of the Act creates the offence of obtaining by false pretence (otherwise known as 419). The offence is punishable under section 1(3) of the Act. A person who commits an offence under subsection (1) or (2) of the section is liable on conviction to imprisonment for a term of not more than 20years and not less than 7 years without option of fine.

The relationship between ATM fraud and Advance Fee Fraud is that a person who commits an ATM fraud can be liable on conviction under section 1(3) of the Advance Fee Fraud Act. If a criminal under the pretest of offering assistance to an ATM user exchanges his non workable ATM card to the valid or genuine card belonging to another ATM user, the criminal then uses the valid or genuine ATM card of the ATM user to withdraw money from the account of the ATM user, this will amount to obtaining by fraud under section 1 (1) of the Act.

An elderly illiterate man who was interviewed said[59]

[54] No. 13 of 1995
[55] Advance Fee Fraud and other Fraud Related Offences (Amendment) Act 1995
[56] Cap A6 Laws of the Federation 2010 (Revised Edition) Note that the National Assembly in 2017 amended the Act referred to as the Advance Fee Fraud and Other Fraud Related Offences (Amendment) Bill 2017 and sent it to the president for Assent. But the president refused to give assent to the bill and sent bank to the National Assembly for clarification of certain issues. As at the time of writing this paper the bill is with the National Assembly.
[57] Okonkwo and Naish*, Criminal Law of Nigeria* (2nd edn, spectrum Books, Ibadan 2012) 309
[58] Advance Fee Fraud and other Fraud Related Offences Act Cap A6 Laws of the Federation 2010 (Revised Edition)
[59] Oludayo Tade (n.50)

> "I was given an ATM card and nobody told me how to use it. Outside the bank, I gave it to a young man at the ATM to help me withdraw cash. He did it and return my card to me. After a few days, I noticed money had left my account which I promptly reported to my bank. At the bank, I was told that the young man had swapped my card."

It is important to point out that ATM users should exercise restraint in giving out their ATM cards to strangers at the ATM Terminal to help withdraw cash for them. These fraudsters often hang around the ATM Terminal to swindle unsuspecting ATM users under the pretext of assisting them to withdraw cash.

Cybercrime (Prohibition Prevention, Etc) 2015

The Cybercrime (Prohibition Prevention, Etc) Act was enacted in 2015. One of the objectives of the Act is to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, persecution and punishment of Cybercrimes in Nigeria. It is therefore, a critical legislation designed to curb cases of cybercrimes including ATM fraud in Nigeria. The Act contains laudable provisions that not only promote cyber security in Nigeria but also check the perpetration of cybercrimes in Nigeria. The few sections of the Act that deal with ATM fraud shall be discussed hereunder.

Identity theft and Impersonation

This involves stealing people's password to enter networks to which they do not have authorization and this may create enormous opportunities for fraud to occur.[60] Identity theft is also a term used to refer to fraud that involves pretending to be someone else in order to steal money or get other benefit.[61]

Identity theft is an offence under the Cybercrimes (Prohibition, Prevention, Etc) Act. Section 22 (2) at the Act provides as follows:

A person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, to

[60] Uwem Udok "An Examination of the E-banking Frauds: The Nigerian Banking Industry in Perspective" (2009) (1(1) *conference Journal of Private and Property Law*, 51

[61] Ebem, Onyeagba & Ugwuonah, "Identity theft and solution. The Nigerian Perspective" *Journal of Internet Banking and commerce* https: www.scholarscentral.org. Accessed on 22-5-2020

i. Gain advantage for himself or another person,
ii. Obtain any property or an interest in any property,
iii. Cause disadvantage to the entity or person being impersonated or another person, or
iv. Avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice, commits an offence and is liable on conviction to imprisonment for a term of 5years or a fine not more that ₦7,000,000.00.

The following are identity theft techniques:

i. email based phishing
ii. short message service(sms) scam and
iii. phone calls related scam

Criminals often visit sites such as truecaller.com, harvest phone numbers and the names of registered owners, sent text messages to these phones numbers, addressing the owners by their first or last names while informing them that their BVN registration was incomplete. They will require them to send some financial information such as ATM Pin, account number and so on to enable then ratify one issue or the other.[62] An unsuspecting customer of the bank who responds to these text messages from the criminals are often swindled and his/her funds in the account fraudulently transferred to unknown accounts in other banks.

One Elijah Joseph John, a former staff of Diamond Bank (now Access Bank) was alleged by a certain Aniebiet Daniel Udeme (a customer with the bank to have moved a sum of ₦400,000 from his (Udeme) account same day the money was deposited. According to Udeme, the unauthorized transaction was reported to the banks but was told that it could not be reversed. Consequently, Udeme petitioned the EFCC. EFCC investigated the petition and it was revealed from the investigation that it was John that moved the fund for personal use by fraudulently activating mobile bank on his phone, using the victims banking details under the pretext that he was assisting the victim in resolving a mobile banking issue. John pleaded guilty to the charge and opted for plea bargain.

The court presided over by Justice Riman convicted John and ordered him to pay a fine of ₦10,000, warning him to always steer clear of crime and to always be of good conduct. In addition, the convict agreed to refund the stolen sum of ₦400,000 to the owner.[63]

Theft of Electronic Devices

[62] Ebem, Onyeagba & Ugwuonah (n.60)
[63] Court convicts Banker for identity Fraud "www.efccnigeria.org.acessed on 22nd May, 2020

It is an offence under the Cybercrime Act to steal an ATM. A person who steals an ATM commits an offence and is liable on conviction to imprisonment for a term of not more than 1 year or a fine of not more than ₦1,000,000.00 or both. Distinction must be made between stealing of ATM card and stealing of ATM.[64] Each carries different penalty on conviction. How can an ATM be stolen. An ATM can be stolen by attacking same with dynamites or solid and gas explosive, remove it from the site and use other methods to gain access to the safe. This usually occurs where the ATM is located in remote or isolated areas devoid of security.

Manipulation of ATM/POS Terminals

It is an offence under the Cybercrime Act to manipulate an ATM machine or point of sales terminals with the intention to defraud. Such a person, if convicted of the offence is liable to an imprisonment for a term of 5years or ₦5,000,000.00 fine or both. Where an employee of the bank is found to have connived with another person or group of persons to perpetrate the fraud using an ATM or Point of Sales (POS) device, the employee shall commit an offence and shall be liable on conviction to imprisonment for a term of 7years without an option of fine.[65]

It is difficult for an outsider to manipulate the ATM machine without the connivance of a staff of the bank. This is because manipulation of the ATM may involve entering the ATM Terminal to remove or install certain devices inside the ATM and this cannot be successfully done without the active connivance of an employee of the bank. Manipulation of ATM terminals may take different forms which have already been discussed. Such manipulation may take the form of installing a device in the ATM with the intention of committing or perpetrating fraud. These include card skimming, card trapping and cash trapping. All these involve manipulating the ATM one way or the other to defraud unsuspecting customers.

Electronic Cards Related Fraud

The Cybercrime Act criminalizes electronic card related fraud in section 33 of the Act. A person who with intent to defraud uses any access device including credit, debit charge, loyalty and other types of financial cards to obtain cash, credit, goods or service commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 or both fine and imprisonment and is further liable to pay in monetary terms the value.[66]

Furthermore, a person uses-(a) counterfeit access device (b) an unauthorized access device (c) an access device issued to another person, resulting in a loss or gain, commits an offence and is liable

[64] Section 15(1) of the Cybercrime Act, 2015
[65] *Ibid*. Section 30(1)
[66] *Ibid* Section 33(1)

on conviction to imprisonment for a term of not more than 7years or a fine of not more than ₦5,000,000.00, and a forfeiture of the advantage or value derived from his act.[67] It is also an offence under the cybercrime Act for a person to steal an electronic card and such a person if convicted is liable to imprisonment for a term of not more than 3years or a fine of not more than ₦100,000.00 and is further liable to repay in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.[68]

The above sections criminalize credit or debit card fraud and it takes many forms, for instance, stealing payment cards, cloning or counterfeiting of payment card or use of credit card number to commit online fraud. Copying credit card number for later use or misuse or in the case of ATM, a fraudulent card stripe reader would capture the contents of the magnetic stripe while a hidden camera would sneak at the user pin are all punishable under the above provisions.

A person who obtains credit card number fraudulently and uses same to gain access to an electronic device to defraud victims commits an offence under section 33(1) of the Cybercrime Act. Also a person who steals ATM cards belonging to other persons and uses same to withdraw money from the account of the person using ATM commits an offence punishable under section 33(2) of the Cybercrime Act. It is an offence punishable under section 33)3) for a person to use counterfeit cards or cloned cards belonging to different cardholders to withdraw money from the account of the victims. Presently, a popular music act in Nigeria is standing trial before the Federal High Court, Lagos for being in possession of counterfeit cards and stolen credit information obtained from websites dealing with buying and selling of stolen credit cards.[69]

Dealing in Card of Another

It is an offence under the Cybercrime Act for a person, other than the issuer, to receive and retain possession of two or more cards issued in the name of different cardholders which cards he knows were taken or retained under circumstances which constitute card theft. A person who commits such an offence is liable on summary conviction to imprisonment for a term of 3years or to a fine of ₦1,000,000.00. The convicted person is also liable to repay in monetary terms, the value of loss sustained by the card holder or forfeit the assets or goods acquired with funds from the account of the cardholder.[70] Also, the case involving the popular music star, he was also alleged by EFCC to be using Access Card number 526711020433662 issued to another person in a bid to obtain

[67] *Ibid*. Section 33(2)
[68] *Ibid*. Section 33(3)
[69] Olamide Fadipe "Nigeria: EFCC Witness says Stolen Credit Card Details Found on Naira Marley's Device" https://allafrica.com/stories/201810240030.html: Accessed on 22-5-2020
[70] Section 34 of the Cybercrime Act, 2015

fraudulent gains.[71] In another case prosecuted by EFCC, some staff of one of the branches of Union Bank Plc conspired among themselves to issue ATM card to an imposter in the name of bonafide customers of the bank. The card was allegedly used to withdraw money from the account of the customers for personal use[72]

Criminal Code and Penal Code

By virtue of section 7(2) of the EFCC Act[73] the EFCC is empowered to enforce any other law or regulation relating to economic and financial crimes including Criminal Code and Penal Code. Under section 46 of the EFCC Act.[74]

> "Economic and Financial Crimes" means the non-violent criminal and illicit activity committed with the objective of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud…"

Therefore, EFCC as a criminal enforcement agency is empowered to investigate and prosecute offences under criminal and penal code with leave of the Attorney General of the Federation. Such offences particularly under the Criminal code include conspiracy, stealing, conversion, forgery and obtaining by false pretence. The EFCC can file charges against ATM fraudsters for the offence of conspiracy,[75] stealing,[76] conversion and forgery[77] under the Criminal Code. Therefore, a person who steals ATM card or connives with others to steal ATM card and defraud the victims can also be charged under the Criminal Code for conspiracy and stealing or obtaining by fraud[78] as the case may be. It is pertinent to state that one of the charges levelled against the popular Nigerian Musician was conspiracy[79]

Money Laundering (Prohibition) Amendment) Act, 2017

[71] *Ibid*
[72] EFCC Twitter https://efccnigeria.org. Accessed on 21st May, 2020
[73] CapE8 Laws of the Federation 2010 (Revised Edition)
[74] *Ibid*
[75] *FRN v Inyang* (2006)2 E.F.C.L.R.P.16 see also section 516 of the Criminal Code Cap C38 Laws of the Federation 2004
[76] *Onwodidwe v FRN* (2006) 49 WRNP.1 See also Section 383(1) &(2) of the Criminal Code Cap C38 Laws of the Federation 2004
[77] *FRN v Ikpe* (2006) 2 EFCCLRP. See also section 419 of the Criminal Code Cap c 38 Laws of the Federation 2004
[78] *Ibid*
[79] Olamide Fadipe (n.68)

The Money Laundering (Prohibition) Amendment) Act[80] (MLPA) makes provision for the laundering of proceeds of crime or illegal act. Though, Cybercrime is not expressly mentioned in the MLPA, proceeds of Cybercrime perpetrated by criminals would appear covered by section 15 of the MLPA which states as follow:

> "(1) Money laundering is prohibited in Nigeria (2) Any person or body corporate, in or outside Nigeria who directly or indirectly (a) conceals or disguises the origin of: (b) converts or transfers, (c) removes from the jurisdiction or (d) acquires, uses, retains or take possession of control of any fund or property, knowingly or reasonably ought to have known that such fund or property is or form part of the proceeds of an unlawful act, commits offence of money laundering under this Act."

It is pertinent to state that the unlawful act referred to in section 15(2) of the MLPA includes fraud, forgery or other criminal act. Since cybercrime including ATM fraud is a criminal act, therefore, proceeds of an unlawful act would include proceeds derive from the commission of any cybercrime including ATM fraud. Proceeds from acts perpetrated by ATM fraudsters are unlawful and when they are laundered the fraudsters are held to have committed the offence of money laundering.[81]

Evidence Act

The problem of proof in electronic banking fraud may constitute a major obstacle in the successful prosecution of ATM fraud which is one of the dimensions of the electronic banking fraud. Hitherto, the existing legal framework was inadequate to deal with cases especially involving the use of computers, word processors, telex machines, internet, and fax machines. The evidence status and admissibility of computer and other electronically generated statement of account or print out, emails, telegraphic transfer, telefax have been issues in controversy[82]

The issue of admissibility of evidence is also crucial to the prosecution of ATM fraud as it has capacity to determine the outcome of a case one way or the other. Thanks to the Evidence Act[83]

[80] 2012

[81] Anyone who violates section 15(2) of the MLPA is liable on conviction to a term of not less than 7years but not more than 17years imprisonment but where it is a corporate body, liability is on conviction to (a) a fine of not less than 100% of the funds and properties acquired as a result of the offence committed; and (b) Withdrawal of licence. Where the body corporate persists in the commission of the offence for which it was convicted in the first instance the Regulators may withdraw or revoke the certificate or licence of the body corporate. See F. Eboibi "Curtailing Cybercrime in Nigeria: Applicable Laws and Derivative Sources" Journals. Ezonwaoho eterc.org/index.ph.d/AFJCLJ/article/view/491

[82] Uwem Udok (n.59)

[83] Felix Eboibi (n.80)

which contains adequate provisions to deal with cases involving electronically or computer generated evidence. The admissibility of electronically or computer generated evidence in electronic banking fraud including ATM fraud is subject to the fulfillment of certain conditions. Section 84 states that such document sought to be tendered must have been produced by the computer from information supplied to it during a period over which the computer was used regularly and functioning properly to store and process information for the purpose of which that document was produced at that particular time, any statement contained in such document shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, in any proceedings.[84]

Institutions for Curbing ATM Fraud in Nigeria

Apart from laws and regulations designed to tackle incidences of ATM fraud in Nigeria, there are also institutions that are charged with the responsibility of combating cases ATM fraud in the banking industry in Nigeria. These institutions some of which are regulatory and supervisory agencies, police the banking industry to ensure that certain guidelines and polices that are released by the relevant authorities, are adhered to, strictly by banks and customers as well as implement government laws and regulations to check fraudulent practices.

There are also other institutions that are set up to initiate the process of investigation and/or prosecution of offenders of the laws and regulations. The prohibition or prevention of ATM fraud in the banking industry is further enhanced through the adjudication processes whereby the perpetrators of ATM fraud are brought before the law courts for prosecution and if convicted, sentenced accordingly. These institutions are as follows:

Central Bank of Nigeria

Section 1(1) of the Central Bank of Nigeria (CBN) Act[85] provides that there is established for Nigeria a body known as the Central Bank of Nigeria. It shall be a corporate entity with perpetual succession and a common seal and may sue or be sued in its corporate name.

The CBN is the apex court of the land and one of the principal objectives of CBN as provided in section 2 of the CBN Act[86] is the provision of a sound financial system in Nigeria. The purpose of establishing the CBN was given judicial recognition in the case of *CBN v Ukpong*[87] where the court of Appeal, Ibadan Division stated that by virtue of section 2 of the CBN Act,[88] the purpose

[84] See section 84(1) (2) & (4). See also section 90(1) a & (d)
[85] 2007
[86] 2007
[87] (2006) 13 NWLR (Pt.998) at 214
[88] 2007

of establishing CBN is for overall control and administration of monetary and banking policies of the federal government. The CBN is actively involved in the supervision of the banking system to ensure satisfactory implementation of the monetary policies of the government in its effort to ensure better life for the general populace. The CBN discharges the following statutory responsibilities to ensure that incidences of ATM fraud are prevented or prohibited or even reduced to the barest minimum in the banking industry in Nigeria.

i. **Issuance of Guidelines, Rules and Standards in the exercise of the powers conferred on the CBN by section 28(i)(b) of the CBN Act**.[89] The CBN is authorized to issue guidelines, rules and standards for the maintenance of adequate and reasonable financial services for the public and to ensure good conduct and management of the financial system. It is in pursuant to these inherent powers that the CBN issued the Guidelines on Electronic Banking in Nigeria and the Standards and Guidelines for the operation of the ATM services in Nigeria. The Guidelines and Standards are designed to ensure the efficiency of ATM services and convenience as well as protection of customers. The CBN ensures satisfactory implementation of these Guidelines and standards to restore confidence and promote a sound financial system in Nigeria.

ii. Establishment of Nigeria Electronic Fraud Forum (NEFF)

The Central Bank of Nigeria in furtherance of its efforts at combating fraud within the banking industry established the Nigeria Electronic Fraud Forum (NEFF) to proffer solutions towards addressing frauds arising from the increased adoption of electronic payment.[90] Based on the directive of the NEFF, it becomes imperative for DMBS and electronic payment services providers to ensure that an effective mechanism for alerts are set up within the Nigerian Banking industry towards managing and reducing successful electronic payments fraud rate in the Nigeria Banking industry.

iii. Establishment of Industry Fraud Desk

The CBN through the Nigerian Electronic Fraud Forum directed all DBMS, MMOS Switches and all payments service providers to maintain a dedicated fraud Desk in their respective organization.[91] The fraud Desk shall be approximately staffed with personnel that have requisite training on emerging fraud trends on various electronic payment channels. It is to be noted that the establishment of the fraud Desk is in compliance with paragraph 3.2 (b) of the Standards and Guidelines on ATM operation in Nigeria.

iv. Imposition of Sanctions

[89] 2007
[90] See CBN circular to all DPM, switches and payment service providers number BPS/DIR/GEN/CIR/02/004 dated June 11, 2015
[91] *Ibid*

An important weapon at the disposal of CBN in performing its role in the prohibition or prevention of ATM fraud is the enforcement of laws, rules and regulations through the imposition of sanctions. Such sanctions include removal of directors/officials or connive who collaborate with fraudsters to commit ATM fraud.

An examination of both the Guidelines on Electronic Banking in Nigeria and that of ATM operations in Nigeria reveals that sanctions in the form of monetary penalties are enshrined therein.[92] But the sanctions are not severe enough to deter intending violators of the Guidelines. In some cases, the sanctions do not provide specific monetary imposition of penalties.

v. Know your Customer

In an effort to curb financial crimes and money laundering, the CBN in November, 2001 issued a circular on customer due diligence otherwise known as Know-Your-Customer (KYC). The circular was aimed at reminding banks of the need to ensure that appropriate procedures and documentation are followed in accepting new customers while closely monitoring the activities of existing customers to avoid banks being used as a heaven for financial crimes. The KYC principle is an effort on the part of the CBN to encourage banks to carry out self-regulation therefore, a bank is expected to know much more particulars of their customers.

Section 3 of the Money Laundering (Prohibition) Act,[93] appears to give legal backing to KYC principles. Under the said section, a financial institution shall verify customer's identity and address before opening an account for a customer as well as issuing a passbook. A customer as well as his identity must present to the bank a valid original copy of an official document bearing his name and photograph, his address and also present original receipts issued to the customer within the previous three months by public utilities.

In practice, banks in a bid to enforce the KYC principle insist that a customer who wants to open an account with them must provide the following, viz, a driver's license or National Identity Card, Power Holding Company of Nigeria electric bill or NITEL Bill (during the time of NITEL). A customer may also be required to present his international passport. It is rather unfortunate that sometimes when these documents are provided by the customer, the financial institution rarely verify these documents as provided under section 3 of the Money Laundering (Prohibition) Act.[94] Consequently, there are cases where fake or forged documents are presented leading to all manners of account opening fraud. Sometimes, the bank employees are involved in the fraud by aiding the customer. This calls for strict monitoring and enforcement of the rules and regulations by the CBN.

[92] See paragraph 5.0 of the CBN standards and Guidelines on ATM Operations in Nigeria
[93] 2012
[94] 2012

Economic and Financial Crime Commission (EFCC)

The Economic and Financial Crime Commission (EFCC) was inaugurated on April 11, 2003 with the swearing in of Mallam Nuhu Ribadu as its Executive Chairman in Abuja, by the then Honourable Minister of Justice and Attorney General of the Federation, Mr. Kanu Agabi. Before the inception of EFCC, the Federal Government of Nigeria had set up the National Committee on Financial Crimes *via* executive fiat which was initially headed by Mr. Ade Ajakaiye, the then Commissioner of Police Special Fraud Unit (SFU) and later by Mr. C.Y Akaya, a Commissioner of Police, when the former was transferred out of the SFU. Upon, the establishment of EFCC,[95] the Executive Chairman, Mallam Nuhu Ribadu formally took over the activities of the defunct N.C.F.C from Mr. C.J. Akaya at a brief ceremony, held at No. 15 A Awolowo Road, Ikoyi, Lagos on May 8, 2003. [96]

The EFCC is established by the Economic and Financial Crime Commission (Establishment) Act. It is a body corporate with perpetual succession and seal. It may sue or be sued in its corporate name and may for the purpose of its functions acquire, hold or dispose of property.[97]

Section 6 of the Act provides that the EFCC shall be responsible for the enforcement and the due administration of the provisions of the Act, the investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, future market fraud, fraudulent encashment of negotiable instruments, computer credit, credit card, contract scam and such other activities. The EFCC is also vested with the co-ordination and enforcement of all economic and financial crime laws and enforcement functions conferred on any other person or authority. ATM fraud is a financial crime and EFCC is empowered by the Act to investigate any complaint of ATM fraud lodged with the commission by any compliment.

Furthermore, the commission after due investigation and a prima facie case is established against the culprit is also empowered by the Act to prosecute the offender by enforcing the relevant provisions of the law pursuant to section 7(f) of the Act. The term "*Any other law or regulation relating to Economic and Financial Crime"* in section 7(f) of the Act also includes the enforcement of the Cybercrime (Prohibition, Prevention, Etc) Act[98] which contains copious provisions aimed at checking incidences of ATM Fraud in the country.

[95] The Act establishing EFCC was first enacted in 2002 and later amended in 2004. The EFCC Act 2004 repealed the EFCC Act 2002. It is now known as the Economic and Financial Crimes Commission (Establishment) Act Cap E8 Laws of the Federation 2010 (Revised Edition)

[96] Uwem Udok "Enforcement of Financial Crime Laws in Nigeria. The Role of Economic and Financial Crime Commission" (2016) 27 (1) *Journal of Banking and Financial Law and Practice,* 35

[97] See section 2 (a) & (b) of the Act.

[98] 2015

The EFCC has been involved in the investigation and prosecution of cybercrime offences like identity theft and impersonation, electronic cards related fraud and dealing in card of another. A notable one is the trial of a popular Nigerian Music artist known as Azeeze Fashola on an 11-count charge of conspiracy, possession of counterfeit cards and fraud. His co-defendant, one Yad Isril was said to be at large. He was arraigned on May 20, 2019 and pleaded not guilty to all 11 counts. He was also granted bail of N2million with two sureties in like sum. According to the charge, the defendant committed the offences in different dates, November, 26, 2018, December 11, 2018 and May 10, 2018. Mr. Fashola and his accomplices allegedly conspired to use different Access Bank ATM cards to defraud their victims. They allegedly used Access Bank number 5264711620433662 issued to other persons in a bid to obtain fraudulent financial gains. He was said to have possessed these counterfeit credit cards, belonging to different card holders, with intent to defraud, and which also constituted theft. Mr. Fashola denied the charges. EFCC had since called the first prosecution witness, Nuru Buhari who testified against the accused and was led in evidence by EFCC counsel, Rotimi Oyedepo. The matter is before Justice Nicholas Oweibo of the Federal High Court Lagos.[99]

Police

The Police play a crucial role in the fight against the perpetration of bank fraud including ATM fraud in the banking industry in Nigeria. To be specific, the police have made enormous contribution in the investigation and prosecution of bank fraud.[100]

The police derive their statutory powers both from the constitution and the Police Act.[101] There shall be established for Nigeria, a police force to be known as the Nigeria Police.[102] The constitution also provides for the establishment of a police force for Nigeria. Section 214(i) of the 1999 constitution of the Federal Republic of Nigeria (as amended) provides as follows:

> "There shall be a Police Force for Nigeria which shall be known as the Nigerian Police Force, and subject to the provision of this section no other police force shall be established for the Federation or any part thereof"

Section 214(2) b of the constitution of the FRN (as amended) further provides thus "*The members of the Nigeria Police Force shall have such powers and duties as may be conferred to them by law"*.

[99] Fadipe (n.68)
[100] Uwem Udok "Law Enforcement and the Banking Industry in Nigeria: Assessing the Role of the Police in Curbing Bank Malpractice" (2015) 22(1) *African update (winter 2015)* https://webccus.ed, 5-15
[101] *Ibid*
[102] Section 3 of the Police Act Cap P19 Laws of the Federation 2004

It has been argued that the establishment of the EFCC as a parallel body to discharge the same function of the police is contrary to section 214(1) of the 1999 Constitution of the Federal Republic of Nigeria[103] (as amended). For instance, section 6(b) of the Act[104] provides that the EFCC shall be responsible for the enforcement and the due administration of the provisions of the Act, the investigation of all financial crimes. Furthermore, the EFCC shall be responsible for the co-ordination and enforcement of all economic and financial crime laws and enforcement functions conferred on any other person or authority. Section 6 of the EFCC Act[105] appears to be inconsistent with section 214(i) of the 1999 constitution of the Federal Republic of Nigeria (as amended) which clearly states that no other police force shall be established for the Federation or any part therefore. But section 6 of the EFCC Act[106] appears to constitute the EFCC as a separate or parallel police force carrying out the same functions of the police.

It is suggested that the 1999 constitution of the Federal Republic of Nigeria (as amended) should be amended to empower the EFCC to specifically undertake the responsibility of co-ordinating and enforcement of economic and financial crimes in Nigeria.[107]

Section 214 (2) b of the 1999 Constitution of Nigeria (as amended) grants the Nigerian Police Force such powers and duties as may be conferred on them by law. Accordingly, the Police Act[108] confers on the police the following statutory duties to perform.

h. The prevention and detection of crime
i. The protection of life and property
j. The apprehension of offenders
k. The prevention of law and order
l. The due enforcement of all laws and regulations with which it is directly charged, and
m. The performance of such military duties within and without Nigeria as may be required of them by or under the authority of any Act.

Arguably, most of the above duties of the police appear to be performed also by another government agency which is the EFCC.

[103] I. Omoruyi "Policing Financial Crimes in Nigeria: A critical Examination of Offences under the EFCC Act, 2002 (2004) 9 (3-4) *Modern practice Journal of Finance and Investment Law, 639*.
[104] Laws of the Federation 2004
[105] *Ibid*
[106] *Ibid*
[107] Udok (n.120)7
[108] Cap 19 Laws of the Federation 2004

The Police is further empowered under the Police Act to conduct prosecution but however subject to the powers of the Attorney-General of the Federation and of the state.[109] In *Federal Republic of Nigeria v Osahon and 7 others*,[110] the Supreme Court held, *inter-alia,* that much as the Police have the authority under the Police Act to prosecute, then the Police officers can prosecute cases up to the highest Court of the land. The Supreme Court further held, that the power of Attorney-General come in for the purpose of undertaking, continuing or discontinuing Criminal prosecutions. This invariably means that the police can prosecute up to the highest court of the land without the fiat of the Attorney-General but however subject to the power of the Attorney-General under section 174 of the 1999 Constitution of the Federal Republic of Nigeria (as amended).

Therefore, where there is allegation of ATM fraud in the banking industry the Police have the duty not only to investigate the allegation but also to prosecute where a *Prima facie* case is established against the accused person who perpetrated the ATM fraud.
As already mentioned in this paper, ATM fraud is one of the forms of Cybercrime and by virtue of section 47(1) of the Cybercrime (Procedure, Prevention etc) Act, which states that[111] *subject to the powers of the Attorney-General, relevant law enforcement agencies shall have power to prosecute offences under the Act.* The term "Law Enforcement Agencies" is defined to include any agency for the time being responsible for the implementation and enforcement of the provisions of this Act.[112] Though the Cybercrime Act does not provide a list of the law enforcement agencies to be charged with the responsibility of implementation and enforcement of the provisions of this Act, the Police by virtue of section 214(2) b of the 1999 Constitution of the Federal Republic of Nigeria (as amended) and sections 4 and 23 of the Police Act[113] are empowered to carry out such functions however subject to the powers of the Attorney-General.

The question arises as to whether the police are well-equipped to investigate and prosecute such cases involving ATM fraud which involves the use of electronic device to perpetrate the fraud. Therefore, the Police need to undergo training and re-training on investigation and prosecution skills, expert evidence, information gathering technology and techniques in crime detection, prevention and control order[114] as well as enforcement of general law.

Judiciary

[109] *Ibid*. Section 23
[110] (2006) All FWLR (Pt. 312) P. 1975
[111] 2015
[112] Section 58 of the Cybercrime (Prohibition, Prevention) Act 2015
[113] Cap P19 Laws of the Federation 2004
[114] Udok (n.120)

The Judiciary is one of the organs of government. It is one of the three arms of government. The constitutional function of the Judiciary is to adjudicate on matters brought before the courts. It is the performance of that constitutional function that extends to adjudication of matters in the banking industry.

Section 6(i) and (2) of the 1999 Constitution of the Federal Republic of Nigeria (as amended) provides as follows:

> 6(1) The Judicial powers of the Federation shall be vested in the courts to which this section shall relate being courts established for the federation.
>
> 6.(2) The Judicial powers of the State shall be vested in the courts to which this section relates being courts established subject as provided by this constitution, or a state

The Judiciary plays a significant role in the fight against cybercrime including ATM fraud in the banking industry in Nigeria. Section 50(1) of the Cybercrime (Prohibition, Prevention Etc) Act[115] confers on the Federal High Court located in any part of Nigeria, regardless of the location, where the offence is committed, the jurisdiction to try offences under the Act. The Cybercrime (Prohibition, Prevention, etc) prohibits an application for stay of proceedings in respect of any criminal matter brought under this Act until judgment is delivered.

CONCLUSIONS AND RECOMMENDATIONS

The Banking Industry in Nigeria has experienced fraudulent practices occasioned by the increase in the number of customers and the deployment of technology to fast-track banking transactions. Fraudsters have devised new techniques in the perpetration of their criminal activities. The use of ATM appears to be one of the means used by the fraudsters in the perpetration of their fraud. In some cases, the bank employees are also either directly or indirectly linked to this fraud. Despite the fact that government and other stakeholders in the Banking Industry in Nigeria have put in place measures in the form of rules and regulations as well as institutions to tackle these fraudulent practices, the banking industry in Nigeria continues to experience these problems thereby posing great risk to the stability of the industry.

It is therefore imperative to adopt more effective and efficient measures to curb the incessant cases of the fraudulent practices with particular reference to ATM fraud in Nigeria. Therefore, the following recommendations are hereby made.

Customer

[115] 2015

i. Customer should cover with his or her hand the ATM keypad while entering the PIN and amount.
ii. Customer should report immediately to the bank if the ATM does not work for assistance.
iii. Customer should avoid asking the help of strangers especially suspicious looking individuals.
iv. Customer should observe carefully or be on the look-out if there is anybody following him or her immediately he or she is done with the ATM transaction.
v. Customer should report to the security department of the bank any experienced ATM fraud or crime.
vi. Customer should be careful when asking a commercial tricycle rider or a taxi to convey him or her to the ATM terminal for withdrawal of money. Such people often hang around the ATM terminal after dropping the customer with the intention to rob him or her after withdrawal.
vii. Customer should desist from sending his or her son, daughter or relative to withdraw money from ATM. It means the customer has compromised his or her PIN number to the person.
viii. Customer should report immediately to the bank any loss of ATM credentials so that the bank can block the account of the customer. Report should also be made to the police.
ix. Customer should read carefully the ATM card application form before signing it.
x. Customer must memorize PIN if he or she writes down PIN on paper then do not keep it in purse or along with the ATM card.
xi. Customer should desist from counting the cash withdrawn from the ATM at the ATM terminal. The counting can be done thereafter at home.
xii. If a customer's ATM card is stuck in the ATM, he or she should not call a bystander to help him or her retrieve the card but should immediately report it to the bank.

Bank

i. Security officers who are not bank staff should not be allowed to deal with customers.
ii. ATM users should be taught to change their Passwords.
iii. Banks should install software that have monitors to monitor the withdrawal pattern of customers to identify and stop suspicious transaction.
iv. There should be internal control measures especially with regard to PIN number generation as it relates to the usage of ATM card, and enabling ATM system to detect and retain cloned cards.
v. Banks should have 24/7 helpdesk where customer can call in the time of distress, especially on weekends, so that the customer's account could be quickly blocked.
vi. Banks should comply with the new charges on ATM released by the CBN with effect from 1st January, 2020. These charges are contained in the Revised Guide to Bank charges.

vii. Banks should not over-charge the customers by continuing to charge the old rates and refusing to send a debit alert for the ATM charges.
viii. Banks should send debit alert for all ATM charges to their customers to enable them know how much they are being charged for ATM withdrawal.
ix. Banks must secure themselves the protection of insurance cover since they may find themselves liable for the payment of money lost due to these frauds.
x. Banks can provide cards containing a microchip that can make them harder to forge.
xi. Banks should regularly embark on anti-fraud education campaigns using indigenous languages considering that some bank customers can't read and write.
xii. Banks should conduct regularly security checks on their ATM and around the location of the ATM.
xiii. Banks should post security personnel to guard the ATM facility and the surroundings at all times.
xiv. Banks should always respond timeously to distress calls, written complaints lodged by customers who are swindled by ATM fraudsters by blocking the customers' accounts.
xv. Banks should give a copy of the duly completed ATM card application form to the customer to enable the customer read and understand terms and conditions applicable to the issuance of the card. In the alternative, the bank officer can read and explain to the customer the terms and condition contained therein.

Laws and Regulations

i. Specific penalties/sanctions should be stated for violation of the guidelines on ATM operations in Nigeria.
ii. The penalties/sanctions should be severe or stringent to serve as a deterrent to intending violators of the guidelines.
iii. There should be strict enforcement of the laws and regulations curbing ATM fraud in the country.
iv. Some of the provisions the Guidelines and Standards require updating to be in tune with modern exigencies.

Institutions

i. More logistic and personnel should be provided to the institutions to enable them carry out their enforcement functions
ii. There should be training and re-training of the personnel of some of the institutions on modern investigative skills.
iii. There should be no delay in the dispensation of justice.
iv. There should be special courts to handle cases relating to cybercrimes