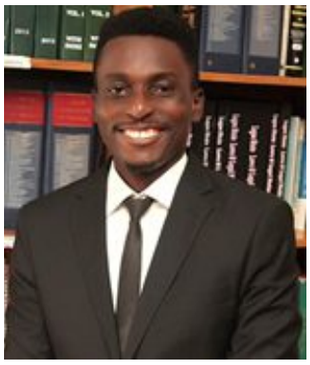
Evaluations: Closing Regulatory Gaps in Security of Electronic Banking Transactions in Nigeria

Thought Leadership | **By Omovefe Oghotomo** June 2018



o.oghotomo@lelawlegal.com

Introduction

It is no longer news that Nigerian banks are continually looking for better ways to improve their service delivery to customers, thereby making banking transactions easy, efficient and more secured. Recent initiatives include the launch of '*ALAT*' (touted as Nigeria's first digital bank) by Wema Bank Plc, '*OCTOPUS*' (reported as an app designed to digitize and consolidate most of the customer's daily activities across multiple devices) by Heritage Bank and many others.[1]

Despite recent innovations, it was reported that fraudsters have, between 2007 and 2017, stolen about N237 billion from Nigerian banks through various electronic and mobile platforms.[2] According *to the Nigerian Electronic Fraud Report 2016*, Nigerians lost N2.19 billion to fraudsters through electronic channels in 2016 fiscal period, with 19,531 reported cases, compared to 10,743 in 2015.The Report also analysed the fraud and the value of losses recorded: Across the Counter Transaction (ACT) accounts for N511.07 million, Automated Teller Machine (ATMs) N464.5million, internet banking N320.66 million and mobile banking transactions, N235.17 million. This shows that losses from 'traditional' channel (ACT) pales into insignificance against its e-counterparts; the trend is likely to be on the increase with greater internet penetration.

With the increased volume of e-payment transactions across Nigeria, there is an urgent need for the Central Bank of Nigeria (CBN) and Financial Institutions (FIs) to constantly evolve measures of ensuring adequate security for such transactions to minimize prospect and actual incidences of e-banking frauds.

This article reviews different forms of e-banking, the need to have robust e-banking regulation in Nigeria and associated issues, including data privacy in the financial sector.

Forms of E-Banking in Nigeria

The various forms of e-banking used by Nigerians includes:

i. **Online/Internet Banking**: This refers to any banking transaction that can be conducted over the internet, generally through a bank website under a private profile. These transactions include services that are traditionally offered at local branches without having to physically visit a branch. Customers can perform financial transactions like paying bills, transferring money from one account to another, etc.

ii. **Mobile Banking:** This allows an individual to perform the same activities using a smart/mobile phone or a tablet. Mobile banking versatility includes using a mobile app, text message banking (Unstructured Supplementary Service Data (USSD)). Virtually all banks are making their sites more mobile friendly, via mobile apps and making upgrades to such apps also to accommodate the needs of customers.

iii. **Automated Teller Machine (ATM):** Interaction with cash dispensing or deposit machines is perhaps the most used form of e-banking in Nigeria and it requires a Personal Identification Number (PIN).

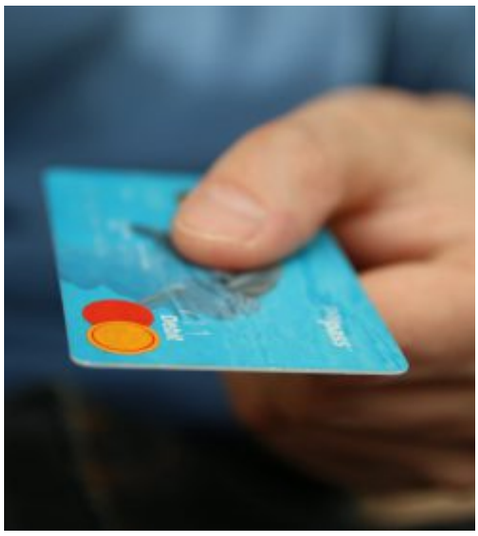
Regulatory Bodies and Legal Provisions for E-Banking in Nigeria

The CBN, the banking sector regulator, is saddled with the responsibility and power to promote and facilitate the development of efficient system for settlement of transactions including the development of the e-payment systems by ***sections 2(d) and 47(2) CBN Act, Cap C4 LFN, 2004***.

Other regulators include ***Nigerian Inter-Bank Settlement System (NIBSS)*** which *inter alia* provides mechanism for same day clearing and settlement of inter-bank transfers and payments; initiating and developing an

[1] *Moses Ashike, 'Heritage Bank Revolutionise Banking Sector with Advanced Intelligent Digital Platform'*, BusinessDay, 11th March 2017 http://www.businessdayonline.com/heritage-bank-revolutionise-banking-sector-advanced-intelligent-digital-platform (accessed 20.5.2018)

[2] *Adeyemi Adepetun, 'Nigerian Banks Lose N237 Billion to Frauds in 10 Years'*, The Guardian,9th November,2017 <http://guardian.ng/business-services/nigerian-banks-lose-n237-billion-to-fraud-in-10-years/> (accessed 9.4.2018)



integrated nationwide network for the electronic or paperless payment, fund transfer and settlement of transactions.

There is also ***National Information Technology Development Agency (NITDA),*** mandated to foster the development and growth of Information Technology (IT) in Nigeria and the ***Nigerian Electronic Fraud Forum (NEFF)*** comprising various stakeholders such as the law enforcement agencies, payment service providers, telecommunication companies, banks, etc. The ***NEFF*** is to: educate and inform all banks and other stakeholders on various electronic fraud issues and trends; proactively share fraud data/information amongst banks and service providers to enable prompt responses to prevent fraud losses; and formulating cohesive and effective fraud and risk management strategies. The NEFF is also to define key requirements relating to e-payment security on behalf of the industry.

The ***Nigeria Deposit Insurance Corporation (NDIC)*** supervises banks so as to protect depositors; foster monetary stability; promote an effective and efficient payment system and promote competition and innovation in the banking system.

In order to ensure the protection of customers' rights in e-transactions, in 2003 the CBN issued ***Guidelines on Electronic Banking in Nigeria (Guidelines)***. The Guidelines sought to address amongst others: information and technology standards on security and privacy, monetary policy, legal guidelines on banking regulators and consumers' rights protection, and regulatory and supervisory issues.

Recently, there has been calls to revise the ***Guidelines*** due to its outdated provisions, given the significant subsequent developments especially with regards to electronic data.

One of its shortcomings is that the ***Guidelines*** did not provide for sanctions on proven violations of its provisions. As part of effort to fill such gaps, in 2015 the ***Cybercrime (Prohibition, Prevention, Etc.) (CPPA) 2015*** was enacted and specifically imposes duties on FIs regarding customers' e-banking protection: ***sections 37-40 CCPA***. For instance, ***section 37 CCPA*** mandates FIs to put in place effective counter-fraud measures to safeguard customers' sensitive information. Any FI that makes an unauthorized debit on a customers` account shall upon written notification by the customer, provide clear legal authorization for such debit to the customer or reverse such debit within seventy-two (72) hours. Failure to reverse such debit within 72 hours, is an offence; the defaulting FI would be liable on conviction to restitution of the debit and a fine of N5 million.

This provision has been reportedly observed more in breach by FIs. An example is where a customer unsuccessfully attempts to withdraw money from an ATM, but the customer is debited. There are instances where a customer writes a letter informing the bank of the unauthorised debit and the bank tells the customer to come back in four (4) working days which is approximately ninety-six (96) hours. There have also been instances of debit reversals taking up to two (2) weeks or more, in clear breach of the timeline provisions.

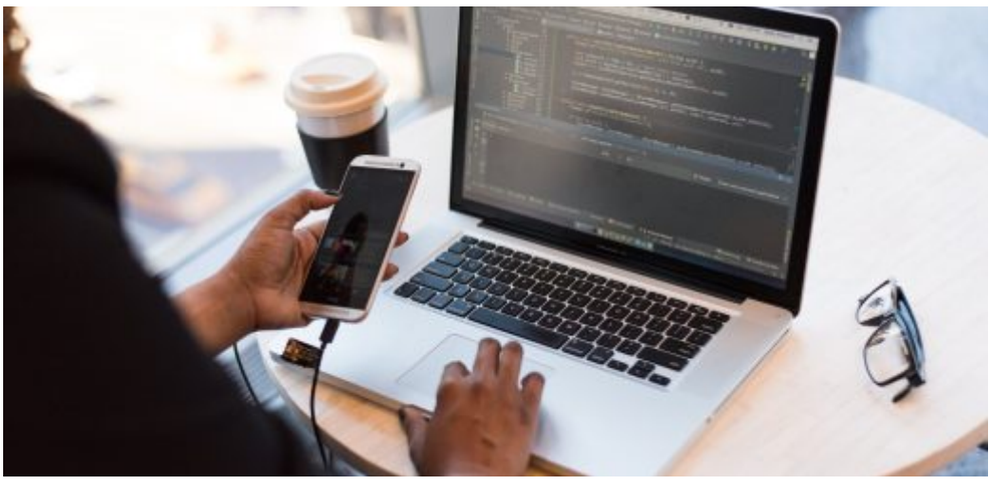
Further, ***section 19(3) CPPA*** makes reference to the fact that the customers have the responsibility of proving FI's negligence, where a financial breach occurs. This is a herculean task given that the evidence of proving same is within the control of the bank. It is comforting that the ***Consumer Protection Framework (CPF) 2016 (para. 2.6.1(5))*** provides that if a breach occurs as a result of the bank's negligence, the bank has to compensate such customer. With the emergence and widespread acceptance of e-banking, associated litigation are also being recorded, especially on unauthorized withdrawal of money from customers' accounts.

An example is ***Agi v. Access Bank Plc.***[3] The Appellant, a business man, maintained a current account with the Respondent at its Markurdi Branch in Benue State. The Respondent issued the Appellant with an ATM debit card. The Appellant activated the card and changed its number to his own secret PIN and used it exclusively. On 3rd October 2009, the Appellant travelled to Onitsha to purchase goods. He drew a cheque of N70,000 payable to himself out of his credit balance of N95,518, but he was informed that he had no funds in his account. He was further informed that the money in his account was withdrawn through ATM transactions at the Respondent`s Fontana Service Station, Enugu. The Court of Appeal held that where a person has custody of an item, it implies that the person in custody is in care and control of it for inspection, preservation and security. In the instant case, the Appellant`s ATM card was in the Appellant`s custody.

Similarly in ***UBA Plc v. Wasiu Bakare***[4] the Respondent paid N140,000 into an account with the Ijebu-Ode branch of the Appellant bank on 2nd June 2008.The Respondent approached the same branch two days later (4th June 2008) for transfer of the money in payment of the school fees of his son, whereupon the Respondent was informed by an employee of the bank that there was no money in the account. At the conclusion of trial, the trial court found that the Appellant failed to substantiate the allegation that it was the Respondent himself or the person he directly or inadvertently revealed his personalised PIN to that transferred the money. The onus of proving PIN misuse was on the Appellant; and this was not discharged. This case is presently on appeal.

Paragraph 1.5 Guidelines on Automated Teller Machine Operations in Nigeria 2016 (GATMON) makes it clear that ***"where the user of an ATM blocks his image for camera capture, the ATM shall be capable of aborting the transaction."*** Though this is a laudable provision, its enforcement is in doubt. There have been instances where people with head and facial covering have successfully used the ATM for transactions. How then do we create a measure of balance in cases of religious and traditional coverings? It would be apposite to introduce Iris based biometric ATM which is presumably more secure than the conventional PIN based ATM due to the fact that it requires biometric verification which is not easily copied, stolen or cloned. Although it impacts the capital expenditure of banks, its use in Japan has reportedly curbed fraudulent activities.[5]

3 [2014] 9 NWLR (Pt. 1411), 121
4 [2017]4 NWLR (Pt. 1555), 318
5 *Erin Oneil, 'ATM Use Biometric to Combat Fraud', The Balance, 20th February, 2018* <http://www.the.balance.com/atms-use-biometric-to-combat-fraud-315794> (accessed 7.4.2018)



The ***CPF (para. 2.6.1(4))*** addressed the issue where an employee aids in the commission of such crime by stating that: ***"Financial institutions shall enforce disciplinary action against employees involved in fraud and report same to the regulator. Where required, the CBN shall blacklist such employee from further employment within the industry."*** On its own part, ***section 20 CCPA*** stipulates seven (7) years imprisonment for such an offence.

The ***Guidelines for Card Issuance and Usage in Nigeria 2014 (GCIU)*** made reference to the destruction of ATM cards in ***para. 4.5.0*** stating that ***"any trapped card in the ATM shall be rendered unusable (by perforation) by the Acquirer and returned to the Issuer on the next working day."*** A practical example is if Mr. A has a card issued to him by Bank Y, and he then decides to use it in Bank Q's ATM, if the card gets trapped, he is required by law to get a new card. Although this move was necessitated to increase ATM Card's security, its application has caused untold hardship on users, given that ATM networks in most rural areas are weak. Rather, card owners should be allowed to retrieve their cards after showing means of identification and the banks can further verify such user through the Bank Verification Number (BVN) database.

"Financial institutions shall enforce disciplinary action against employees involved in fraud and report same to the regulator. Where required, the CBN shall blacklist such employee from further employment within the industry."

Data Privacy in the Banking Sector

Developments in the area of ICT has made private information a valuable commodity, which if not carefully protected, can be used for unlawful purposes. The global financial sector is in possession of significant customers' data in respect of their financial activities especially e-banking transactions therefore leading to a high risk of these information being breached.[6]

In 2014, the CBN introduced the BVN and the idea was to have a unique biometric identity which will be assigned to every account holder. While this was initiated to reduce cyber-crime, there was no specific regulation for BVN until 2017 when the ***Framework for BVN Operation and Watch list for the Nigeria Financial System*** (***FBOWNFS***) was issued. Although electronic fraud is prevalent, it was reported to have drastically reduced by 38% over the last two years. The ***FBOWNFS*** provides for security and data protection of banks customers alongside ***CPF`s*** in ***Paragraph 2.6.2***. The ***FBOWNFS*** **in Paragraph** ***1.8(i - iii)*** states that: ***"Parties involved in BVN operations should put in place secured hardware, software and encryption of messages transmitted through the BVN network; BVN data are to be stored within the shores of Nigeria and not to be routed across borders without CBN's consent; Users of BVN information should establish adequate security procedures to ensure the safety of its information".***

The ***FBOWNFS*** might be a step in the right direction for FIs, but there are no specific provisions in relation to the acceptable eight (8) principles for data protection. An example is the principle that the institution collecting data should ensure that it is adequate, relevant and not excessive. Thus, when a customer is opening a savings account, the FI should not seek employment information as this will only be relevant if the customer is seeking credit facilities.

One of the major gaps in ***FBOWNFS*** can be seen in ***Paragraph 2.3.2*** where a bank is given the option to continue/ discontinue banking with those on the watch list. Arguably, this should not be the case. Once an individual's name appears on such list, then the individual should not be allowed to transact any business with that bank whatsoever; and if the person was erroneously put on the list, then such an individual ought to be adequately compensated. This would arguably instil due diligence in the banking sector.

Conclusion

The laws and regulations touching on security of e-banking transaction in Nigeria have to some extent achieved its aim. Relevant stakeholders (sectoral regulators, FIs, law enforcement agencies, etc.) and government must forge mutually beneficial initiatives to stem the tide of fraudulent activities in the e-banking system. This would further bolster the confidence of many unbanked Nigerians and could serve as a springboard for accelerating financial inclusion across Nigeria.

LeLaw Disclaimer:

Thank you for reading this article. Although we hope you find it informative, please note that same is not legal advice and must not be construed as such. However, if you have any enquiries, please contact the author, Oghotomo Omovefe at o.oghotomo@lelawlegal.com ***or*** *email: info@lelawlegal.com.*

[6] *Jim Marous, '8 Steps to Improve Bank and Credit Union Cross Selling', The Financial Brand, 6th August, 2014* <http://thefinancialbrand.com/39865/banks-and-credit-unions-must-improve-cross-selling/> (accessed 7.4.2018)

[7] *Elizabeth Adegbesan, 'Losses to E-Fraud Declines by 38%', Vanguard, 18th December, 2017* <https://www.vanguardngr.com/2017/12/looses-e-fraud-declines-38/> (accessed 9.4.2018)

[8] *Banking And Payments Federation Ireland: Data Protection Guide May 2013* states the eight principles which includes obtaining and processing data fairly, processing it only for one or more specified, explicit and lawful purpose, use and disclose it only in ways compatible with the purposes for which it was obtained ,keeping it safe and secured, keeping it accurate, complete and up-to-date, ensuring that it is adequate, relevant and not excessive, retaining it no longer than is necessary for the specified purpose, give a copy of his/her personal data to an individual on request.