Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.100, 2020

Cashless Policy and Consumer Protection: A Critical Appraisal of the Nigerian Cyber Laws

Ifeoluwa Etomilade-Oduola
Research Fellow, Department of International Law, Nigeria Institute of Advanced Legal Studies, Lagos, Nigeria

Abstract
This article in discussing the transitioning of Nigeria to a cashless economy, considers the regulatory framework in place to protect consumers from cybercrimes that surfaced with the policy. A critical appraisal of the existing cyber laws in Nigeria showed consumers have been left in the loop, whilst the law has failed to effectively protect bank consumers from the onslaught of cybercrimes which accompanied the cashless policy. An analysis of the consumer protection framework especially those issued by the Central Bank of Nigeria revealed inadequate protective mechanism for consumers whilst the required standard for compliance by banks has been evasive. Amongst the recommendations given is the need to specify the standards required for banks for effective consumer protection while a specified body should be created to ensure strict compliance. This article concludes by emphasizing that even though a cashless economy is of immense benefit, there is need for banks to put appropriate infrastructures in place that will shield its consumers from cybercrimes and enhance consumer confidence in financial institutions generally.
Keywords: Cashless Economy, Bank Customers, Cybercrimes, Cyber laws, Central Bank of Nigeria, Consumer Protection.
DOI: 10.7176/JLPG/100-02
Publication date: August 31st 2020

1. Introduction

Over the years there have been series of reforms in the financial industry by the Central Bank of Nigeria (CBN) aimed at ensuring the industry not only meet up with international best practices and the nation's vision 2020 but also protect consumers, the recipients of this policy. Part of the reform was the introduction of the cashless policy, which saw a reduction but not a total removal in cash flow. Most if not all developed countries operate a cashless economy, which predominantly involves the payment for goods and services through an electronic medium, this however does not mean a total elimination of cash as money will continue to be a means of exchange. This economic policy is designed to enhance and fast track payment services by breaking down the traditional monetary means of exchange Nigerians are familiar with as well as foster financial stability.

Prior to introducing this cashless policy, the financial industry was bedeviled with long queues at different financial institutions, frustrated customers, bad customer relations, slow and tedious payment process, coupled with insufficient cash to cater for customer's demands amongst others. In other to deal with these challenges, CBN introduced a cashless policy to reduce the volume of cash used for business transactions, encourage E-banking thereby reducing cash handling costs by banks, financial crime as well as provide the platform it needed meet up with international best practices as well as attain the vision 2020.

The benefits notwithstanding, this new policy came with its own complications and challenges which were not adequately prepared for. Operating a cashless policy effectively required using up to date technology and electronic gadgets which requires reliance on infrastructures like power supply, internet facilities, public literacy etc. It is however unfortunate that these infrastructures were neither fully put in place nor was there any plan in motion to remedy the anomalies identified prior to implementing the policy in other states.

The policy instead of alleviating the problem of corruption, money laundering, and financial terrorism amongst others aggravated the problems with the fear of possible loss of money through fraud, scamming, cloning of website particularly online banking sites, cyber theft etc. due to poor or non-availability of facilities to ensure its effectiveness and adequate protective mechanism.

The regulatory framework presently operative in Nigeria focused more on reforming the financial sector to achieve the vision 2020 with little or no focus on how to effectively protect the recipients (bank consumer or customers) of the reform from vices that has arisen or will arise in the future like other countries do.

Based on the foregoing this article will consider the movement from cash to cashless economy through its historical analysis. The second part will discuss the benefit of the cashless policy and the challenges, while the third part will analyse the policy as it pertains to the concept of consumer protection. The regulatory framework of cybercrime in Nigeria will be discussed in the fourth part with the types of cybercrimes. The fifth part will deal extensively on the pitfalls of the Nigeria cyber law through a critically analysis of the flaws of the act as it relates to consumer protection. The article will in concluding make recommendation on the need for consumers to be adequately protected under the cashless policy in the sixth part.

1.1 Conceptual Clarification

This section defines some of the concepts used in this article for ease of understanding of in the rest of the article. Cybercrimes- Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Consumer- means every person or organization that enters into computer based purchase, lease transfer, maintenance and consultancy service agreements with a computer service provider and the customer and agent of the consumer. Consumers will also include bank account holders who carry financial cards, cyber or internet users. For the purposes of this paper, the term consumer and customer are used interchangeably to have the same meaning.

1.2 Historical Perspective of Cash to Cashless Economy

Prior to introducing the cash-less policy, the Nigerian economy relied heavily on cash for exchange of goods and services, which saw Nigerians keeping cash in their houses rather than bank it. This exposed many to the risk of theft, loss of money through negligence or fraud, spendthrift while this cash flow further aided money laundering, bribery and corruption. The fear of bankruptcy discouraged those bold or literate enough from putting all their monies in a bank, while many Nigerians trusted their monies with thrift contributors (alajo or esusu) because of their accessibility.

Over the years the Nigerian banking industry has been clogged-down by unfair competition from foreign banks, inadequate capital, mismanagement and lax regulations, which prompted the introduction of various phases of reforms. The 2008 global financial crisis further exposed the weaknesses of the banks as well as the unethical deeds going on within the management, this propelled the need to introduce other new reforms to improve the financial stability of banks and the quality of services rendered for overall economic growth.

Banking reforms generally involves a regular introduction of rules and regulations by the Central Bank of Nigeria to guide the operation of financial institutions in ensuring the effective running of other banks, geared towards national economic growth and also attaining international best practices. These reforms are aimed at ensuring consumers are satisfied and protected from scrupulous bank activities especially when quality of services rendered influences the country's integrity at the international level.

Being the apex bank, the Central bank of Nigeria (CBN) plays a supervisory and regulatory role over other banks, coupled with the power to introduce reforms needed to ensure the banking sector perform their functions effectively. Even though the CBN have been introducing reforms intermittently in the past for the advancement of banks, the cashless policy not only affected the banks, but also consumers especially with the introduction of electronic channels for deposit or withdrawal of money.

2. Benefit of Cashless Policy and Its Challenges

Through the 2011 circular of the CBN, the cashless policy aims to curb excessive dependence on physical cash by Nigeria, curb corruption, embezzlement, money laundering and also assist in the effective implementation of other policies introduced for economic growth. Other advantages of operating a cashless economy under the policy include;

a.) Helping to reduce the cost of banking services, the risk of using cash and the cost of cash usage. Traditionally banking in Nigeria prior to the introduction of the cashless policy, was essentially paper based which gave room for unbalanced accounts, error or delay in payment as well as fraud. The shift from the norm has reduced the costs and hazards associated with operating cash based economy thereby improving the effectiveness of monetary policy decisions aimed at driving economic growth.

b.) Managing inflation and general usage of cash- With the cashless policy, inflation can be relatively managed while cash usage to a large extent is being moderated by discouraging cash transactions and also setting daily cumulative withdrawals and deposits for both individuals and companies from the bank with a penalty fee to be charged for any extra withdrawals.

c.) Helps to reduce corruption, money laundering and embezzlement. Over the years transactions through physical cash have encouraged corruption especially in the political sphere of Nigeria where 'Ghana must go bags' or 'brown envelope' changes hands.

d.) Reduction in cash related crimes like robbery and increased banking convenience for consumers.

e.) Ease of cash transaction and monitoring.

f.) Increased tax revenue- the move towards a cashless economy will imperatively assist the government in ensuring individuals and companies pay promptly thus increasing the tax revenue.

As much as operating a cashless economy would be of immense benefit to Nigerians, there are challenges associated with it that needs to be addressed. They include;

a. Literacy-The level of literacy in Nigeria is a source of concern especially in a country where there is

high level of illiteracy. Having a high level of illiteracy would result in too much dependence on the few literate which may leave them at the mercy of these scrupulous few.

b. Public Confidence- Financial institutions need to regain the confidence of Nigerians especially, those with past unpleasant financial experience. Also the benefit of the cashless policy must be evident in order to encourage Nigerians considering the low banking level.

c. Security- To guarantee the success of the scheme in Nigeria, the problem of security needs to be addressed especially when internet scam is on the rise.

d. Automatic Teller Machines (ATM) – Although the ATM is not a cashless device, however various forms of cashless transactions like funds transfer, paying for airtime and utility bills can be done through the ATM. This has helped in reducing queues in the banking hall; however network failure has continued to sabotage this initiative by the CBN. Similar problem of slow or network failure from internet service providers like MTN, Glo, 9mobile etc. pose a problem to other cashless schemes like mobile wallet , internet and mobile banking introduced by various financial institutions in addition to the ATM.

e. Point of Sale Terminals (POS) - operating a cashless economy requires having POS terminals at most if not all retail outlets. Low or connectivity failure of bank networks constitute a drawback to the policy, consumers are forced to resort to handling physical cash even for big outlets with POS terminals.

f. Unstructured Market- the problem of unstructured market is another challenge militating against the success of the policy. Without a proper structure in place that will accommodate the Nigerian situation and peculiarity, the Nigerian economy would never be ready to advance like other developed countries operating a cashless economy.

g. Power-irregular power supply has plagued the country eons, whilst failure to address this problem is affecting the effectiveness of the cashless policy.

h. Constant Access - to enjoy the 'supposed' benefit of operating a cashless economy, onsite and offsite, consumers must be able to access bank services.

i. Hidden Charges- Although operating a cashless economy has a lot of benefits, financial institutions are however using it as an avenue to exploit its customers through hidden bank charges for banking services with little or no protection.

Based on the aforementioned, to effectively and successfully operate a cashless economy like other developed countries, all the challenges clogging its success must be addressed.

3. Cash-Less Policy and Consumer Protection

With the introduction of the cashless policy, transacting at the cyberspace through electronic devices became necessity, however at a cost to consumers who became exposed to cybercrimes (or computer related crimes) like spamming, cloning, phishing, identity theft etc with little or no regulatory framework in place to protect consumers. Various existing laws on consumer protection would now be considered;

a. Consumer Protection Council Act 1992

Although the 1992 Nigerian Consumer Protection Council Act (CPC) identified a consumer as an individual, who purchases, uses, maintains or disposes of products or services while section 6 of the Act provides avenue for redress where a consumer suffered a loss, injury or damage as a result of the use or impact of any goods, product or however the act neither provided for consumers of services offered by financial institutions nor specified any remedy for such consumers especially on issues pertaining to cybercrimes.

Also a perusal of the entire Act revealed the act only relates to products and services that pertains to human health and not to services being offered by the financial industry as such the 1992 Act cannot be relied on by consumer of financial products seeking redress or compensation. Pursuant to the powers conferred on it by the 1992 Act, the Consumer Protection (Products and Services Monitoring and Registration) Regulations 2005 was introduced by the CPC. The Regulation made the registration of products manufactured, imported, advertised, sold, distributed in Nigeria mandatory, however it made no mention of products relating to financial services.

b. Nigeria Deposit Insurance Act 2006

The Nigeria Deposit Insurance Act (NDIA) was established to insure the deposit of consumers, although it provides some level protection for consumers, however it is clear from section 2(1) (a-c), that the Act can only be relied on in cases of imminent danger or actual financial difficulties of an insured financial institution bank. The Nigeria Deposit Insurance Corporation is the body charged with preventing damage to public confidence in the banking system and guaranteeing payments to depositors, however, the extent to which the NDIC protection will come into play is dependent on one hand on evidence of financial difficulty of a bank or revocation of license and cybercrime on the other hand is not a proof of such difficulty that would warrant the intervention of NDIC. Furthermore, the maximum amount provided for in section 20 would seem small when compared to monies lost to cybercrime, this further shows that the protection provided by the NDIC even if it is applicable to victims of cybercrime would be too small to mitigate the hardship being faced.

c. Consumer Protection Framework 2016

The Central Bank of Nigeria (CBN) in recognition of some of the current deficiencies, introduced the Consumer Protection Framework (Framework) in 2016, pursuant to its powers under the CBN Act and the BOFIA to address the issue of consumer protection to be followed by banks to ensure that consumers of financial services are protected and treated fairly. This framework will focus on consumer protection through onsite examination and off site supervision. The CBN is also to ensure financial services operators put in place effective consumer risk management framework by supervising the financial institution's (FI's) rate of compliance.

The framework further identified the existence of rights between the bank and the consumer which would not only serve as the bedrock of the relationship but would also boost public confidence in the FIs. Aside the right to be rightly informed and educated through public awareness , the consumer protection framework also stipulates that a consumer has a right to choose from the variety of products offered by a FI with a right to opt out in case of dissatisfaction; right to redress, right to safety ; right to confidentiality and right to fair treatment.

The CBN framework further identified the need for appropriate measures to be taken by the banks for adequate consumer protection especially on issues like

i. Data Privacy i.e. Contact details, account number and balance, statement of accounts.
ii. Fraud.

The above shows good intentions, however the onus is still on the financial institutions (FIs) to put measures in place whilst the standard required may differ from one bank to the other based on what is considered 'sophisticated', the question is which of the measures to be adopted will give consumers utmost protection especially when the CBN only specify minimum technology standards for payments platforms only. A perusal of the CBN consumer framework showed amongst other duties, the need for FIs to perform periodic internal risk assessment to identify and assess data security risks on their systems. The framework however did not specify which body would be responsible for ensuring absolute compliance of the FIs with these specified duties.

The framework having recognized consumers of financial services are vulnerable and needs to be protected, it however trivialized the issue of risk management and did not recognize that through the cashless policy, consumers are exposed to different types of risks that seem not to be within the purview of why the framework was introduced. The framework should have focused more on how consumers particularly e-consumers will be protected from risks associated with all cybercrimes.

The supervisory role performed by the CBN when examined neither indicated measures to be taken to ensure strict compliance nor did it specify the standards (or level of standard) to be followed for the duties imposed on these FIs in the framework. This shows the CBN only performs general supervisory role through the committee specifically created for that purpose.

It is worthy of note that despite having a 'seemingly' detailed framework, the rate of cybercrime has not reduced neither are consumers free from risk associated with some banking services, this shows that this guideline has not fully solved the problem.

Reports from the 2016 and 2017 Nigeria Cyber Security watch showed increased loss of monies by banks by virtue of fraud through electronic channels and across the counter transaction as against the 2015 report. This loss is clear evidence that the guideline itself is not sufficient neither is it an adequate tool to be relied on by banks to escape various risks bank customers are vulnerable to. Also being a guideline, which serves as a guide, does not have a binding status like an enacted law, but being a document to be read in conjunction with the CBN Act and other subsidiary legislation, FIs may still be obliged to comply with the framework.

The Bank Verification Number (BVN) introduced by the Nigerian Central Bank though another attempt at resolving the problem of e-banking fraud and other related offences, has done nothing to totally eradicate cybercrimes, as the BVN is only required for over the counter withdrawals with the person being physically present whilst it is neither requested nor required, for persons engaging in e-banking or e-transactions as such any person with access to the internet can engage whether legally or otherwise in e-banking without the 'supposed' security the BVN provides.

Aside from the failure of the BVN to effectively secure customer's e-transactions, the increase in fraud cases and internet banking crimes in Nigeria can also be attributed to the collusion cooperation of the staffs of banks with the fraudsters.

4.0 Regulatory Framework of Cybercrime in Nigeria

In aligning herself with international best practices through the introduction of the cashless policy, Nigerians were exposed to all forms of cybercrimes whilst the existing regulatory framework was not well suited to combat the menace or protect Nigerian consumers. This lacuna created an enabling environment for these cybercriminals to escape the hand of justice. The existing laws which seem to prohibit cybercrime include the 2002 Economic and Financial Crimes Commission (Establishment) Act (EFCC Act), Evidence Act 2011, Advance fee Fraud and other Fraud Related Offence Act 2006 and the Money Laundering Prohibition Act 2011.

These Acts are now examined to determine their potency or otherwise in combating cybercrimes in relation

to the cashless policy in Nigeria for the purpose of consumer protection.

4.1 Economic and Financial Crimes Commission (Establishment) Act 2004

The Act established the Economic and Financial Crime Commission (the Commission), charged with the responsibility of investigating all financial crimes including advance fee fraud money laundering, counterfeiting, illegal charge transfers and the prosecution of other offences relating to financial crimes in section 6(b). Cybercrime though not amongst the crimes specifically identified in the Act, can be situated within the Act, being an economic and financial crime which involves an account holder and financial institutions whilst the illegal acquisition of wealth by cyber criminals is in itself a fraudulent Act (section 6-18).

Various sections of the act including section 5(2) (b) has been relied on by the commission in many instances to secure convictions in cases involving former governors and public office holders which is usually done in collaboration with other government bodies within and outside Nigeria on various issues including the recovery of proceeds or forfeiture of properties acquired through corruption, financial crime or other related offences.

Even though cybercrime can be situated within the Act, the implementation of the 2015 Cybercrime Act and empowerment of the Attorney General of the Federation to effectively prosecute cybercrimes and cyber security matters more or less took cybercrime out of the scope of the crimes they can prosecute, although the process of recovering proceeds of such crime can still be situated within the powers of commission. This means consultation with the office of Attorney General of the Federation is essential to the effective performance of the commission's duty.

In effectively performing its duties, the commission has encountered various challenges ranging from lack of cooperation from other anti-graft agency to the presumed duplication of functions due to the unlimited power given to the commission by section 7(f) which is the root cause of friction between it and other law enforcement agencies like the ICPC.

Another problem which may hamper the operation and effective performance of the commission is the task of collecting all reports relating to suspicious financial transaction and analyzing them to determine the response to be given to the reporting agency. The Commission may due to these volumes of reports it receives be restricted without adequate time to make its own in investigation into activities which might have been overlooked even though grievous.

Based on the foregoing, it is evident the Act though suitable to curb other financial crime like corruption and money laundering is not particularly suited to tackle cybercrime. It is worthy of note that internet fraud is just a fraction of what cybercrime is all about as such the Act in its present state cannot effectively curb cybercrime particularly when the focus of the commission seem to be more on the prosecution and recovery of proceeds of corruption from corrupt public office holders. With a limited focus on cybercrime and more focus on recovery of proceeds, consumers would still be exposed to cybercriminals.

4.2 Money Laundering (Prohibition) Act 2011 Amended.

The Money Laundering (Prohibition) 2011 is another law that makes provisions to prohibit the laundering of monies derived from an illegal act or crime which slightly relates to cybercrime. Proceeds from an illegal act such as bribery and corruption fraud, internet scam, e-banking theft etc. are usually invested in a legal business in order to conceal the origin. Section 17 and 18 not only recognizes the culprits and accessory (ies), such person(s) would also be punished, as such a bank employee who aids a cybercriminal in accessing customer's account without consent would be punished.

Furthermore, the act neither provided nor imposes on any person the responsibility or duty to report any suspected money laundering transactions to any of the agencies mentioned in the act for local transaction even though such exists for international transactions. As such there is no obligation on the part of any person approached for such illegal transaction similar to those stated in section 2 to report to the appropriate authorities where the transaction is a domestic transaction that may or may not exceed the stipulated amount stated in section 1.

Through the Act, Financial institutions (FIs) are empowered to do special surveillance of account in certain accounts (see section 6 (1) (a-d)). FIs may however be handicapped by lack of the wherewithal to monitor all these accounts to determine which transaction might look suspicious or not. Also in subjecting only certain accounts to surveillance based on the conditions stated, the possibility of overlooking other accounts that may be proceeds of money laundering is high.

Also in situations where a cybercriminal illegally accesses and transfers money through e-banking to an untraceable offshore account, FIs may through this be incapacitated to either retrieve this money or make a report to the commission of the alleged fraud.

Despite the provision on special surveillance, money laundering may still be perpetuated even if none of the conditions specified is met, particularly if there are insiders colluding with these criminals, it is therefore important to increase the threshold for determining money laundering transactions.

A perusal of the act also showed that consumer protection is not part of the scope of the provision that is majorly concerned about proceeds of a crime being sanitized or 'cleaned' to disguise their illicit and unlawful origins. To conceal the origin of funds, the money must have been illegally acquired through illegal means like cybercrime. This means a consumer must have been defrauded either because there is no protection or the existing protection is not effective enough to ward off cybercriminals. The illegal act must have been performed before detection or an investigation on the source of the money is commenced.

This in essence means the 2011 is not specifically enacted to protect consumers and avoid fraud although an inference of consumer protection though limited can be made on section 6 since such act may help to promptly detect illegal activities before other consumers become victims. It should also be noted that the present money laundering act is traditional in nature and is not entirely a computer based crime to which cybercrime is related as such there is a limit to which the money laundering act can be effectively used to curb cybercrime as well as protect consumers. It is therefore imperative for the present money laundering act to clearly reflect technological advancement to capture proceeds of all crimes without limit on the amount that can be flagged (section 1).

4.3 Advanced Fee Fraud and Other Related Offences Act 2006

The Act was enacted to prohibit and punish offences pertaining to advance fee fraud and other fraud related offences like cybercrime and online frauds especially when software is used not only to mask the identity of the perpetuator but also use information obtained through the internet to commit fraud on an online account (section 2).

Section 7 also makes 'any person who conducts or attempts to conduct a financial transaction which involves the proceeds of a specified unlawful activity, with the intent of promoting the carrying on of a specified unlawful activity' would be liable upon conviction to a fine of N1 million or forfeiture. Where the criminal is an insider within the financial institution or corporate body or any other person, such person would be liable to imprisonment not more than 10 years and not less than five years.

The Act in combating cybercrime vests the responsibility of monitoring unlawful activities on banks, internet service provider and cybercafé. One cannot but wonder how these players can effectively monitor cybercriminals especially cybercafé where data of users of the café facilities are usually not kept and for how long such record should be retained if by any chance they are kept? The requirement that all cybercafés operators and ISPs should monitor the use of their systems and keep a record of transactions made by users though laudable, might make users vulnerable to exploitation or identity theft if this data/information gets into the hands of criminals.

This requirement would need a review when Nigeria enacts privacy protection law to protect data collected in Nigeria from unnecessary disclosure. Presently section 37 of the amended 1999 constitution law is the only law that expressly recognizes the right to privacy of persons in Nigeria. It however does not cover data that are gotten in today's digital age.

4.4 Nigerian evidence Act 2011

Prior to the repeal of the 1945 Evidence Act, admissible evidence in court were limited to documentary evidence as stated in sections 84 and 93. The limitation of the Act coupled with failure to envisage technological advancement and its vulnerability to exploitation made prosecution of cybercrimes difficult if and when such criminals are arrested and put on the stand. It should be noted that much importance is attached to evidence in court proceedings as it is the yardstick by which the veracity of oral testimony is tested. With the documentary evidence limitation, cases involving cybercrime might be discarded on this basis, with many accused escaping prosecution because the evidence available for the offence charged were electronic and the court neither recognize nor accept such.

In recognition of this lacuna, the 1945 act was repealed in 2011 to recognize and accept both digital and electronically generated evidence subject to the conditions stated in subsection 2 of section 84. The non-satisfaction of these conditions may result in the rejection of any document derived from a computer and as well as affect the admissibility of any direct oral testimony which the electronic evidence may intend supporting. This clearly shows that the rule for the admissibility of documentary evidence is still being followed under the Evidence Act 2011 irrespective of the origin of the document being tendered before the Court of Law to support an oral testimony (section 83).

Irrespective of the benefit of this addition to the cause of fighting cybercrime, the act's major objective is to assist prosecutors in ensuring justice is served to cybercriminals during trial. This is a clear indication that consumer protection is outside the scope of the act because the act is generally required after the fact (when the crime has been committed) not before the fact (prior to the commission of cybercrime). This is therefore a case of medicine after death on one hand, since the essence and benefit of section 83-84 is grasped when a conviction is made while consumers on the other hand are the ones to bear the brunt of the cybercrime and the lack of effective protection.

4.5 Cybercrimes (Prohibition, Prevention, Etc.) Act 2015

From the foregoing discussion, it can be deduced that the legal framework regulating cybercrime in Nigeria is inadequate to effectively regulate cybercrime more so the laws were not unified. This informed the enactment of the 2015 Cybercrimes Act is to regulate the conduct of persons in the cyberspace and cybercrimes in Nigeria. Through this Act, the regulatory framework became unified with its focus strictly on cybercrime, thus making the prosecution of cybercriminals easier.

4.5.1 Types of Cybercrimes/Computer Related Crimes under the 2015 Act

Although several offences can be classified under cybercrime in sections 9, 11, 23(1), 24 & 25, however this part with restrict itself to crimes that directly affects consumers of financial services. They include;

a. Cyber Terrorism

It is an act of terrorism committed through the cyberspace (section 18). It involves gaining unlawful access to information stored on the computer or the network by the government or organization with the intention of using such information to either intimidate or manipulate to advance a political or social goal. Section 1 of the Terrorism (Prevention) Act 2011 defines act of terrorism as an act which is deliberately done with malice and may seriously harm or damage a country or an international organization.

b. Unlawful interception/Hacking (section 12)

It involves the illegal interception of communications between users either through emails or other forms of transfers in order to record the information exchanged while hacking refers to the use of technology to gain unauthorised access to a computer system, program, or data for the purpose of exploration or for causing damage once inside.

c. Computer forgery and fraud - this can be in form of e-banking fraud (sections 13 & 14).

d. Identity theft and impersonation (sections 58 & 22).

It is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone else and uses it for his own personal benefit. This many involve opening a fictitious website or cloning the website of a bank with intent of obtaining access to the sensitive information of unsuspecting individuals.

e. Phishing, spamming and Computer virus

Phishing is an attempt by a phisher to fraudulently retrieve legitimate users' confidential or sensitive information like passwords and usernames by mimicking electronic communications from a trustworthy or public organization in an automated fashion. To access confidential information illegally, viruses, Trojans, worms and other software can be sent into a computer unaware. These viruses when sent to a system have a potential of accessing and destroying valuable information. Spamming refers to the indiscriminate use of electronic messaging systems to send unsolicited bulk messages like spam mails, online ads etc.

f. Theft of electronic devices like phones and laptops with sensitive information (section 15).

Unlawful access to a computer is considered a crime in section 6(1) and punishable with a term of imprisonment of not less than two years or to a fine of not less than five million naira or to both fine and imprisonment. In cases where a person accesses computer unlawfully with the intent of obtaining and securing access to any computer data, program, commercial or industrial secrets or confidential information, such person shall be liable to a term of imprisonment of not less than three years or to a fine of not less than seven million naira or both.

The Act in section 7, further provides that any person, who intentionally and without authorization or in excess of authority intercepts any data from a computer, from a connected system or network commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than five million naira or to both fine and imprisonment. This provision exists not only to secure information stored on the internet and privacy of Nigerians but also protect data collected over the years from unlawful access and usage.

In ensuring effective prosecution, section 21 requires internet and phone service providers to retain and make available to government agencies customer information, including traffic data as well as subscriber information when requested. Failure of a provider to cooperate with government agencies when customer information is requested, would attract a fine of at least N10 million, while its director/manager/officer would be prosecuted and, on conviction, be subject to at least three years in prison and/or a N7 million fine.

Section 19 of the Act imposes a duty on financial institutions to safe guard sensitive information of their customers and prohibits them from giving a single employee access to sensitive information.

Section 19(3) provides that financial institutions must mandatorily put in place effective counter - fraud measures to safeguard their sensitive information, where a security breach occur the duty to prove negligence lies on the customer to establish that the financial institution in question could have done more to safeguard its information integrity.

This burden might be difficult to discharge in the face of lack or insufficient information of the internal workings of the financial institution to help the customer determine affirmatively whether the bank, neither would the customer know and the measures that was put in place to safeguard his information.

5. Pitfalls of the Cybercrime Law vis. a vis. Consumer Protection.

Looking at the objective of the 2015 Act, it is evident that the primary focus of the act is the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria, while applauding these objectives especially in the face of cyber insecurity occurrence around the globe, it is however tactless to have a law prohibiting an act in place without making provisions for specific ways/means the vulnerable stakeholders can and should be adequately protected through deliberate actions/steps of the financial institutions (FIs).

More alarming is the fact that aside requiring FIs to use a proxy with firewalls, neither the CBN guideline nor the Act specify any strict uniform standard to be followed in protecting consumer data even though section 19(3) provides that financial institutions must as a duty to their customers put in place effective counter-fraud measures to safeguard their sensitive information. What is considered effective looking at section 19(3) is subjective in nature, because what is effective to one bank might not be to another, as such there is need for the law to specify the type of safeguard to be used by all banks, thus leaving consumers to the whims and caprices of the FIs. As such a FI can decide to fulfill the minimum requirement stated in the guideline without bothering to take additional steps to protect e-consumers from cybercrime.

Placing the burden of proof of negligence on the consumer/customer is evidently another pitfall of the Act. The Act through this provision showed it neither acknowledges nor recognize the need for the law to protect consumers. The effect of this provision is that a FI can even though negligent go scot free where the consumer is unable to proof such negligence.

This obvious gap leads to the question of whether FIs in Nigeria actually have a secured network operated by the bank itself and not by a network provider. Do FIs put additional protection/authentication particularly for consumers operating online accounts?

Being a global threat, in order to effectively tackle cybercrime, there would be a need for international collaboration amongst countries of the world to tackle cybercrime. Based on this, the 2015 Cybercrime Act empowered the Attorney General in section 52(1-2), to seek mutual assistance with or without any bilateral or multilateral agreement; the possibility of a foreign country obliging the request for assistance in the absence of an agreement is unlikely.

Presently, Nigeria is not a signatory to any cybercrime convention, which makes international cooperation harder. The ripple effect is that foreign cybercriminals not resident within the country can perpetuate their evil deeds and still go scot free (section 50 (1) (a-d) (Prohibition, Prevention, Etc.) Act 2015). Obviously the consumer will bear any loss experienced from unlawful access.

Section 7(1) requires cybercafés to maintain a register of users through a sign-in register that should be made available to law enforcement personnel whenever needed. This requirement would make consumers vulnerable if such information gets into a wrong hand, also the personal security of such consumer is at stake. The Act also failed to mention the type of information that should be included in a sign-in register and the duration for keeping and disposing of such register, knowing that a cybercafé cannot keep a register forever. Also keeping a sign-in register and making it available on request is a breach of the consumer's data privacy right (see Bank Limited v. Fathudeen Syed M. Koya1 [1990 - 1993] 5 NBLR p. 368 at 387)

Presently Nigeria does not have any specific law with data privacy or data protection as its main focus. The only mention of privacy right which is in its general term can be found in section 37 of the Nigerian 1999 constitution amended. The section is more of a personal right than a right relating to protection of data. Other laws such as Consumer Code of Practice Regulations 2007, the National Information Technology Development Agency guidelines and the Child Rights Act No. 26 of 2003 are either industry specific, targeted towards some persons considered vulnerable or guidelines that are not mandatory for private companies and only serve as a reference point for data collectors.

The 2011 Freedom of information Act 2011 (the FOI Act) though an act on information, is more concerned with ensuring members of the public have access to information and public records. The Act however recognizes there are limits to this right in certain circumstances such as the requirement of consent of a person whose personal information is contained in the information requested or where such information is subject to various forms of professional privilege conferred by law (section 14 &16). Through the exception in sections 14&16, the FOI recognizes the right of privacy and data protection of individuals in Nigeria.

Furthermore several offences were identified and criminalized, however the mode of enforcement of these provisions was not stated in details nor explicitly stipulated. Section 47 further provides that relevant law enforcement agencies shall have power to prosecute offences under the Cybercrime Act without expressly stating the particular agency/body that would be responsible for such prosecution.

6. Recommendations and Conclusion

Having identified the benefits of operating a cashless economy in Nigeria, the problem of cybercrime that bank customers are exposed to particularly for e-transactions and the pitfalls of the 2015 Cybercrime Act introduced to address the problem of cybercrime, this paper makes the following recommendations that will guarantee adequate

protection for bank customers in Nigeria;

a. The CBN guideline on electronic banking is very inadequate particularly for cybercrimes, as such there is need for the CBN to elaborate more on the standard required on security issues associated with the deployment of software by FIs. Also the guideline needs to be converted into a subsidiary legislation for it to have a binding status.
b. The provision on proof of negligence needs a review that will show that the Act was enacted to protect consumers and not give FIs leeway to be negligent.
c. The Act needs to specify the duration for keeping details of cybercafé customers as required by the law and also state clearly the type of information to be recorded keeping in mind the need to also guarantee the security of such customer. In order to ensure data collected by cybercafé and FIs are not misused, there is need to enact a privacy Act in Nigeria.
d. The Act needs to expressly state the agency/body that will be charged with the duty of enforcing the provisions of the cybercrime Act and also ensuring strict compliance.
e. Consumer protection should be one of the core objectives of the Act and not just detection, prohibition and punishment. Without mandating the FIs to have up to date international standards facilities in place to secure consumers, the only thing the 2015 Act would be good at is detecting and punishing cybercriminals, while the level of cybercrime will continue to increase in Nigeria.
f. To achieve the vision 2020, measure up with international best practices and also effectively eradicate cybercrime, it is imperative for Nigeria to not only be a signatory to the 2001 Budapest Convention but to also champion the adoption and ratification of a criminal policy similar to the convention in West Africa. The convention's preamble not only recognizes the need to protect personal data of individuals but is also convinced that the policy will serve as deterrence against breach of confidentiality of computer data by criminalizing such conduct (Article 2-6 Budapest Convention 2001). With the adoption of such policy by Nigeria along-side other existing cybercrime laws, financial institutions and service providers would be under strict obligation to ensure that both consumer data and transactions are adequately protected against cybercrimes (Article 5-6 Budapest Convention 2001). Its ratification will also enhance investigation and prosecution of cross border cybercrime considering that cybercrime cuts across borders.
g. There should be a yearly summit on cybercrime, Cyber security and consumer protection as follow up and constant reminder on the need for every FIs to ensure its consumers are effectively protected by securing its web.
h. Where appropriate and necessary, legislation should be enacted to address aspects that may have been omitted to clear any doubt or ambiguity or to address any lacuna. With respect to 2015 Act and the concept of consumer protection, there is need enact a subsidiary legislation for that purpose.
i. There is need to design a counter measure like an internet security framework that will promptly detect online fraud.

Consumer satisfaction should be the utmost focus of the 2015 Cybercrime Act and this can be achieved only if the Act focuses more on actually protecting consumers of services rendered by the financial institutions like banks by including provisions that is evidently centered on this objective. The Act as it is presently is focused on the crime and the criminal with a provision that seem to favor FIs against the consumers who is required to prove negligence of the bank in case of a suit against the bank. To effectively protect consumers in Nigeria, it is imperative that the recommendations proffered in this paper be applied.

References

1. Chawki M., Darwish A., Khan M.A., Tyagi S. (2015), '419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria, 593 *Cybercrime, Digital Forensics and Jurisdiction. Studies in Computational Intelligence*, Springer, 129-144.
2. Taiwo, J.N., Ayo Kehinde Oluwafemi Afieroho Evawere & Agwu M. E, (2016) 'Appraisal of Cashless Policy on the Nigerian Financial System', 16(1) *West African Journal of Industrial and Academic Research,* 2
3. Osazevbaru, Henry Osahon &Yomere, Gabriel, (2015) 'Benefits and Challenges of Nigeria's Cash-Less Policy, 4 (9) *Kuwait Chapter of Arabian Journal of Business and Management Review*, 2.
4. Odior, S. E. and Banuso, B. F., (2012) 'Cashless banking in Nigeria: challenges, benefits and policy implication', 8 (12), *European Scientific Journal*, 289-316
5. Dugeri, M., 'Cashless Economy in Nigeria: Issues, Challenges and Prospects' (2013), <https://mikedugeri.wordpress.com/2013/03/21/cashless-economy-in-nigeria/> accessed 25 September, 2017.
6. Yaqub J. O & Others, (2013), 'The Cashless Policy in Nigeria: Prospects and Challenges' International Journal of Humanities and Social Science, 3(3) International Journal of Humanities and Social Science, 206-2011.
7. 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, p.5, < www.uncjin.org/Documents/congr10/10e.pdf>, accessed 2 April, 2019.
8. Baiden, John E., (2011) 'Cyber Crimes' *SSRN*, 1 <https://ssrn.com/abstract=1873271> or

<http://dx.doi.org/10.2139/ssrn.1873271> accessed 6 December, 2019.

9. P.V.C.Okoye & Raymond Ezejiofor, (2013) 'An Appraisal of Cashless Economy Policy in Development of Nigerian Economy', 4 (7) *Research Journal of Finance and Accounting*, 239.
10. Aniekan Akpansung & Matthew Gidigbi, (2014) 'Recent Banking Reforms in Nigeria: Implications on Sectoral Credit Allocation andEconomic Growth'5 (13*) International Journal of Business and Social Science*, 92;
11. Ordu Monday Matthew & Anyanwaokoro Mike, (2016) 'Cashless Economic Policy in Nigeria: A Performance Appraisal of the Banking Industry'18(10) *IOSR Journal of Business and Management*, 2.
12. Central Bank of Nigeria Act 2007, see also Statement of CBN Core Mandate < http://www.cbn.gov.ng/aboutcbn/> accessed 28 May, 2018.
13. Capital market, 'CBN Unveils Four Pillars of Banking Reforms',<https://www.proshareng.com/news/Capital%20Market/CBN-Unveils-Four-Pillars-of-Banking-Reforms/9523> accessed 28 May, 2018. Ajayi L.B, 'Effect of cashless monetary policy on Nigerian banking industry: Issues, prospects and challenges' 2014 IJBFMR 2, 29. < http://www.bluepenjournals.org/ijbfmr/pdf/2014/November/Ajayi.pdf> accessed 30 May, 2018.
14. Ajayi L.B, (2014) 'Effect of cashless monetary policy on Nigerian banking industry: Issues, prospects and Challenges' 2 *IJBFMR*, 29-30. < http://www.bluepenjournals.org/ijbfmr/pdf/2014/November/Ajayi.pdf> accessed 30 May, 2019.
15. Central Bank of Nigeria, 'Industry Policy on Retail Cash Collection and Lodgement, Ref: COD/DIR/GEN/CIT/05/031' < https://www.cbn.gov.ng/OUT/2011/CIRCULARS/COD/RETAIL%20LODGEMENT.PDF> accessed 30 May 2019.
16. Kpefan, Ochei Ailemen, (2012) 'Fast Tracking Business Transactions Though A Cashless Economy in Nigeria: Benefits And Challenges' *The Nigerian Banker* April-June, 12.
17. Kara Scannell (2013) 'Cybercrime without a Trace' *Financial Times* (United States, 31 May) < https://www.ft.com/content/c30bd528-c9d5-11e2-af47-00144feab7de> accessed 5 June 2018.
18. Adekoya, F. " Cashless Economy: The Many Hurdles Before CBN, The Guardian, Lagos, 2011, 22nd June; p .23, accessed in Kpefan, Ochei Ailemen (2012) , 'Fast Tracking Business Transactions Though A Cashless Economy In Nigeria : Benefits And Challenges' The Nigerian Banker, 15.
19. Central Bank of Nigeria, 'CBN Consumer Protection Framework' CPD/DIR/GEN/CPF/03/004, < https://www.cbn.gov.ng/out/2016/cfpd/consumer%20protection%20framework%20(final).pdf> accessed 1 November 2019, 21.
20. Ifeanyi Onuba 'Banks Lost N219bn to fraudsters in 2016 – CBN' *Punch Newspaper* (Nigeria, 31 May 2017) <http://punchng.com/banks-lost-n2-19bn-to-fraudsters-in-2016-cbn/> accessed 7 June, 2018.
21. Abiola Odutola, (2018) 'Nigerians loseN200bn to e-fraud, cybercrimes in 9 months' *The Point* (Nigeria, 15 November), < http://www.thepointng.com/nigerians-lose-n200bn-to-e-fraud-cyber-crime-in-9-months-investigation/> accessed 7 June, 2019.
22. Bamidele Ogunwusi, (2018) 'Nigeria: BVN as Antidote to Bank Fraud in Nigeria' *All Africa* (Lagos, 8 March), <http://allafrica.com/stories/201503092062.html> accessed 25 October 2017.
23. EFCC media and publicity, 'EFCC Secures 703 convictions in 3 years- Magu' EFCC (Abuja, November 12, 2018) < <http://efccnigeria.org/efcc/news/3424-efcc-secures-703-convictions-in-3-years-magu> accessed 26 February 2019.
24. Ethelbert Okey Lawrence, (2016) ' Economic and Financial Crimes Commission (EFCC) and the Challenges of Managing Corruption in Nigeria: a Critical Analysis'6(4) *International Journal of Scientific and Research Publications*, 341,
25. Uglor S, (2006*), Evidence: Text and Materials*, (2nd edition) Thomson Sweet: Maxell, 187.
26. Yagarta, B.N, (1998) *Documentary Evidence: The Law, Practice and Procedure*, Jos University Press Ltd, 48.