TILBURG LAW REVIEW
Journal of International and European Law

Uchenna Jerome Orji, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria' (2019) 24(1) *Tilburg Law Review* pp. 105–124. DOI: https://doi.org/10.5334/tilr.137

RESEARCH ARTICLE

Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria

Uchenna Jerome Orji*

This paper[1] examines the consumer protection regime under the Nigerian Cybercrimes Act with a view to assessing the extent to which it protects consumers from cybercrime in the banking and financial sector. It finds that the regime is not adequate as it does not place sufficient obligations on banks and financial institutions to safeguard the personal information of their customers from unauthorized access. Additionally, the findings suggest the absence of an explicit regime for determining liability for unauthorized payment transactions in situations where a consumer's electronic banking or payment information is compromised. The article also highlights examples of legal regimes in Europe and the United States that could be adopted in order to strengthen the consumer protection regime under the Act. Finally, some challenges impeding the protection of consumers from cybercrime in the Nigerian banking and financial sector are pointed out along with proposed responses to address them.

Keywords: Consumer protection; Cybercrime; Electronic Banking and Payment Services; Banks and Financial institutions; Nigeria

1 Introduction

Nigeria currently has the largest population of internet users and mobile telecommunications subscribers in Africa.[2] Data released by the Nigerian Communications Commission (NCC) in 2018 indicates that Nigeria had over 100 million internet subscribers,[3] and over 150 million mobile telecommunications subscribers.[4] However, increasing internet penetration and telecommunications access in Nigeria has had implications on the rise of cybercrime in the country. In particular, there has been a growing trend in the perpetration of cybercrime such as phishing, electronic card fraud, Automated Teller Machine scams, hacking, malware attacks, identity theft, denial of service attacks,[5] and Business Email Compromise fraud.[6] A report by a non-governmental organization, Paradigm Initiative Nigeria, estimates that the annual and potential cost of

* LL.B (Hons.), (University of Nigeria); LL.M (University of Ibadan); PhD (Nnamdi Azikiwe University Nigeria); Barrister and Solicitor of the Supreme Court of Nigeria, jeromuch@yahoo.com

[1] The article was presented at the International Conference "The Responsible Consumer in the Digital Age. International and Nordic Perspectives on Financial Consumer Protection", organized in 2018 by the Centre for Enterprise Liability, Faculty of Law, University of Copenhagen, with the support of the Carlsberg Foundation, the Dreyers Fond and the Romanian Embassy to the Kingdom of Denmark and Iceland.

[2] *See* Internet World Stats, *Nigeria Internet Usage and Telecommunications* Reports (December, 2017) <https://www.internetworldstats.com/stats1.htm> accessed 5 November, 2018.

[3] *See* NCC, 'Internet Subscriber Data' (May, 2018) <https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-table-5> accessed 5 November, 2018.

[4] *See* NCC, 'Telecommunications Subscriber Data' (May, 2018) <https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#|view-graphs-table-5> accessed 5 November, 2018.

[5] *See* Craig Rosewarne and Adedoyin Odunfa, *The 2014 Nigeria Cyber Threat Barometer Report* (Wolfpack Information Risk and Digital Jewels 2014) 51–56.

[6] *See* Symantec Corporation and African Union, *Cybercrime & Cybersecurity Trends in Africa* (Symantec Corporation and African Union 2016) 15.

cybercrime to the Nigerian economy is over 13 billion US dollars.[7] One sector that has been affected by the growing trend of cybercrime in Nigeria is the banking and financial services sector. In this regard, both banking and financial institutions as well as their customers have repeatedly been targets of cybercrime activities.[8] Despite this development, however, the Nigerian government appeared slow in providing an elaborate legal response that will ensure the protection of consumers.[9] Finally, in 2015, the Cybercrimes (Prohibition and Prevention) Act[10] was enacted to criminalize cybercrime and provide for the protection of critical information infrastructure. The Act also introduced a range of provisions aimed at protecting the users of electronic banking and payment services from cybercrime. This paper seeks to examine these consumer protection provisions with a view to assessing the extent to which they can effectively protect consumers in the Nigerian banking and financial sector from cybercrime. The paper observes that the Act's consumer protection regime is not adequate as some of its provisions, such as section 19(3), do not place sufficient obligations on banks to safeguard the personal banking information of their customers. It also identifies the absence of a liability regime on unauthorized payment transactions where a consumer's electronic banking or payment information is compromised. Additionally, the article highlights comparative examples of legal regimes that protect consumers of electronic banking and payment services in technologically advanced jurisdictions such as the European Union and the United States, with a view to identifying lessons that could be adopted in order to strengthen the consumer protection regime under the Cybercrimes Act. To this end, some tentative reform proposals to the Act are put forward. Finally, the paper points out some general challenges impeding the protection of consumers from cybercrime in the Nigerian banking and financial sector and proposes responses to address them.

The article is organized as follows. The remainder of this first section will discuss the meaning of the terms 'cybercrime' and 'consumer protection', including an overview of the essence of consumer protection in electronic banking and payment services. It will also provide a background on the Nigerian banking and financial sector. The second part will then focus on the development of Nigeria's legal response to cybercrime, and most notably the Nigerian Cybercrimes (Prohibition and Prevention) Act of 2015. The third section will analyze selected provisions of the Act that aim to protect consumers of electronic banking and payment services from cybercrime. Subsequently, the fourth section will discuss some challenges impeding the protection of consumers from cybercrime in the Nigerian banking and financial sector and propose appropriate responses. Finally, the main findings are summarized in the conclusion.

1.1 Cybercrime

There is no universally accepted legal definition of cybercrime or computer crime. Generally, 'cybercrime' or 'computer crime' are often used interchangeably to refer to instances where digital technologies are either the target of a malicious or unlawful activity or the instrument for facilitating a crime or malicious activity. Thus, 'cybercrime' (or computer crime) is used as an umbrella term to refer to all forms of crime perpetrated with the help of computer resources, regardless of whether the final target is a computer resource itself or not.[11] Cybercrime has also been defined as "computer-mediated activities which are either *illegal or considered illicit* by certain parties and which can be conducted *through global electronic networks*".[12] Accordingly, the term is used to describe a range of offences including traditional computer crimes, as well as network crimes.[13] However, there are different views as to the most appropriate legal definition of what constitutes 'cybercrime' or 'computer crime'.[14] Generally, cybersecurity laws tend to avoid such explicit definitions.[15] In this paper, cybercrime will be used to broadly refer to electronic crimes that target users of electronic banking and payment services including phishing, electronic card fraud, Automated Teller Machine scams and hacking of bank accounts.

---

[7] *See* Gbenga Sesan, *et al*, *Economic Cost of Cybercrime in Nigeria* (Paradigm Initiative 2013) 11.

[8] *See* Segun Akintemi, 'Electronic Banking Frauds: An overview', *The Nigerian Banker* (July–September, 2015) 9–12.

[9] S*ee* Uchenna Jerome Orji, *Cybersecurity Law and Regulation* (1st edn, Wolf Legal Publishers 2012) 487–561.

[10] *See* Cybercrimes (Prohibition and Prevention, etc) Act 2015, s 1.

[11] *See* Lambiotte Guillaume, 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges', *Virus Bulletin Conference* (September, 2009) 63.

[12] *See* Chris Hale, 'Cybercrime: Facts and Figures Concerning the Global Dilemma', (65)6 *Crime and Justice International*, (2002)18. (Emphasis added).

[13] *See* Gercke Marco, *Understanding Cybercrime: A Guide for Developing Countries* (ITU 2009) 17.

[14] S*ee* Orji, (n 9) 17–19.

[15] *See* for *e.g.*, The African Union Convention on Cyber Security and Data Protection (Malabo, 2014), and the Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

1.2 The Concept of Consumer Protection

Before defining the concept of 'consumer protection' it appears imperative to first consider the meaning of a 'consumer'. The *Blacks Law Dictionary* defines a 'consumer' as "a person who buys goods or services for personal, family or household use, with no intention of resale [or] a natural person who uses products for personal rather than business purpose".[16] Another definition states that a 'consumer' is a "[person] who uses or requests a service for non-business use and would include someone not contractually bound to the supplier".[17] The Nigerian Consumer Protection Council Act defines a 'consumer' as "an individual who purchases, uses, maintains or disposes of product or services".[18] Thus, in generic terms, a 'consumer' refers to an 'end-user' of goods or services. In the banking and financial services context, a 'consumer' or 'customer' would then mean any person who subscribes to or uses the services of a banking or financial institution. Such services may include deposit, savings, credit, debit, money transfer, or electronic banking and payment services.

'Consumer protection' refers to the "act of safeguarding the interests of the consumer in matters relating to the supply of goods and services".[19] Accordingly, the concept of consumer protection is generally used to classify measures that seek to ensure that consumers are fairly treated and that their rights are protected in commercial transactions that involve the supply of goods or services. The basic rights of a consumer include:

(a) *The right to safety*: this requires that consumers are to be safeguarded against goods or services that are defective or risk prone;
(b) *The right to information*: this implies that consumers are to be informed adequately with respect to the accurate price, as well as the quality, or quantity of goods or services;
(c) *The right to choice*: this implies that consumers are to be provided with a wide variety of goods or services to choose from;
(d) *The right to be heard*: this entitles consumers to make complaints and receive a response from the suppliers of goods or services;
(e) *The right to seek redress*: this implies that consumers are entitled to seek redress for their complaints in complaint resolution forums;
(f) *The right to consumer education*: this requires that consumers are to be educated about their rights, as well as the products or services they wish to purchase; and,
(g) *The right to compensation*: this implies that a consumer should be compensated appropriately by a supplier when a product or service is found to be defective.[20]

Generally, the concept of consumer protection aims to prevent the suppliers of goods or services from taking advantage of consumers while also ensuring that consumers obtain redress for defective goods or services. Consumer protection promotes market competition by keeping unfair market practices that affect consumers in check. In legal literature, it is usually explained and justified with the concept of the 'weaker party'.[21] This is because consumers are considered to be weaker than their contracting partners and are assumed to have an inferior bargaining power in contractual arrangements.[22] Another argument supporting consumer protection is that consumers are less knowledgeable than service providers about products and services they wish to purchase, and therefore require some level of protection.[23] The concept of consumer protection is characterized by laws, regulatory measures and the activities of State and non-State actors that seek to safeguard the rights of consumers while dealing with suppliers of goods and services. The laws that govern consumer protection are broadly classified as 'consumer protection law(s)'.[24]

---

[16] *See* Bryan A. Garner (ed), *The Black's Law Dictionary* (9th edn, West Publishing Co 2009) 358.

[17] *See* Ernie Newman, 'Consumer Protection and Telecommunications', in Ian Walden (ed) *Telecommunications Law and Regulation* (OUP 2012) 455.

[18] *See* Consumer Protection Act 1992, s 32.

[19] *See* Felicia Monye, *Law of Consumer Protection* (Spectrum Books Ltd 2003) 19.

[20] *See* United Nations Guidelines for Consumer Protection (as expanded in 1999) (2003), paras II and III.

[21] *See* Giesela Ruhl, 'Consumer Protection in Choice of Law', (44) *Cornell International Law Journal* (2011) 571.

[22] *Ibid.*

[23] *Ibid.*

[24] *See* Uchenna Jerome Orji, *Telecommunications Law and Regulation in Nigeria* (Cambridge Scholars Publishing 2018) 252.

1.3 Essence of Consumer Protection in Electronic Banking and Payment Services

Generally, the essence of consumer protection is underscored by the need to prevent suppliers from exploiting the vulnerability of consumers. This need appears to arise from reasons including the disparity between the bargaining power of the consumer and the resources of the supplier, and the disparity between the knowledge of a supplier and that of the consumer with respect to a particular product or service. There is also the assumption that suppliers, given their expertise and knowledge, can manipulate demand and prices to the detriment of consumers and further diminish the ability of consumers to make choices. With respect to electronic banking and payment services, the essence of consumer protection arises from the need to ensure that consumers have a high degree of trust in the use of such services, and thereby promoting the adoption and sustained use of electronic banking and payment systems and platforms in conducting financial transactions. Thus, consumer protection in electronic banking and payment services particularly aims to guarantee the protection of consumers' basic rights by ensuring that consumers are protected from acts such as unauthorized electronic access to their accounts or personal financial information by either service providers or unauthorized third parties, and that service providers and liable third parties will be held to account where such rights and security requirements are breached.

1.4 The Nigerian Banking and Financial Services Sector and Cybercrime

The Nigerian banking and financial services sector comprises twenty two major commercial deposit money banks,[25] as well as special investment banks and community banks, and non-bank financial institutions.[26] The sector is regulated by government institutions including the Central Bank of Nigeria (CBN) and the Nigeria Deposit Insurance Corporation (NDIC). In particular, the CBN is responsible for regulating and supervising the commercial activities of banks and financial institutions,[27] and also has a consumer protection unit that manages complaints made by consumers against banks and financial institutions,[28] while the NDIC is responsible for insuring the deposit liabilities of Nigerian banks and supervising insured banks.[29] Aside from the CBN and the NDIC, government agencies such as the Economic and Financial Crimes Commission (EFCC) and the Consumer Protection Council (CPC) have mandates that apply in the banking and financial sector. For example, the EFCC can investigate financial crimes such as cybercrime in the banking and financial sector,[30] while the CPC can take measures to protect consumers in the sector.[31] Thus, in light of the above regulatory landscape of the Nigerian banking and financial sector, it can be discerned that there are multiple government institutions and agencies whose powers and regulatory mandates apply in different aspects of the sector.

In 2018, estimates from the CBN indicated a relatively low patronage of banking and financial services in Nigeria, with only about 53 percent of Nigeria's adult population utilizing banking and financial services, while about 37 percent of the country's adult population are unbanked.[32] This low patronage has been traced to factors such as stringent account opening requirements and procedures, concerns over poor services, the absence of banks and financial institutions in rural areas, low levels of financial literacy, and cultural norms.[33] However, for over a decade, the CBN has been taking steps to increase the population of Nigerians that make use of banking and financial services by implementing policies that promote financial inclusion. For example, in 2003, the CBN began to modernize the payment services system by granting approvals to

---

[25] *See* Central Bank of Nigeria, 'List of Financial Institutions/Commercial Banks' (August, 2018), <https://www.cbn.gov.ng/supervision/Inst-DM.asp> accessed 5 November, 2018.

[26] *See* Central Bank of Nigeria, 'Financial Institutions', available at <https://www.cbn.gov.ng/supervision/finstitutions.asp> accessed 5 November, 2018. *See* Monetary Policy Department of the Central Bank of Nigeria, *The Nigerian Financial System at a Glance* (Central Bank of Nigeria, March 2017) 3–5.

[27] *See* Banks and Other Financial Institutions Act, 1991 (As Amended) s 1, 2, 3, 5, 31–39. *See* s 1(3) and 2(d) Central Bank of Nigeria Act, 2007, *Official Gazette of the Federal Republic of Nigeria* (1 June, 2007) 94, Government Notice No. 34, A63–19.

[28] *See* Central Bank of Nigeria, 'Complaints Management', available at <https://www.cbn.gov.ng/Supervision/cpdcomgt.asp> accessed 5 November, 2018.

[29] *See* Nigeria Deposit insurance Corporation Act 2006, s 27–32.

[30] *See* Economic and Financial Crimes Commission (Establishment) Act 2004, s 6 (b)–(h).

[31] *See* Consumer Protection Council (CPC) Act 1992, s 2.

[32] *See* Dipo Olowookere, 'CBN Admits Failing to Reduce Nigeria's Unbanked Population', *Business Post* (6 June, 2018) <https://www.businesspost.ng/2018/06/24/cbn-admits-failing-reduce-nigerias-unbanked-population/>; Obinna Chima, 'Report: 53% of Nigerians in Banking System – Ericssion', *Thisday* (3 March, 2016), <https://www.thisdaylive.com/index.php/2016/03/03/report-53-of-nigerians-in-banking-system/amp/>; Chike Onwuegbuchi, 'CBN Puts Unbanked Population @ 37%', *Nigeria Communications Week* (23 June, 2018), available at <https://www.nigeria communicationsweek.com.ng/cbn-puts-unbanked-population-37/> accessed 5 November, 2018.

[33] *See* U Kama and M Adigun, 'Financial Inclusion in Nigeria: Issues and Challenges', (45) *Central Bank of Nigeria Occasional Paper* (August, 2013) 26–28, 31–34.

some commercial banks to introduce electronic banking services such as electronic funds transfer services, debit and credit cards, internet banking, mobile banking and Automated Teller Machines (ATM).[34] In 2007, the CBN launched the Payments System Vision 2020 to promote a wider range of electronic payment services such as Point of Sale (PoS) Terminals.[35] In 2011, the CBN also issued the Industry Policy on Retail Cash Collection and Lodgment (IITP/C/001),[36] also known as the Cashless Policy. The policy aims to enhance the development of a cashless economy in Nigeria by reducing the high usage of cash for financial transactions and promoting the use of electronic payment channels as well as the financial inclusion of persons that do not utilize formal banking channels.[37] Following the implementation of the cashless policy, the volume of transactions via electronic banking and payment channels has increased by over 100 percent.[38] Reports from Nigeria's National Bureau of Statistics indicate that there is an increasing adoption of electronic banking and payment services by consumers, including ATM and PoS terminals.[39] However, the overall acceptance of these technologies among Nigerian consumers is still relatively low. For example, a survey conducted by the National Bureau of Statistics found that despite a high ownership of debit cards, only 3.1 percent of consumers preferred to use card/PoS terminals for the payment of goods and services.[40]

Some of the major factors that appear to be responsible for this slow adoption of electronic banking and payment channels include low levels of consumer literacy, consumer protection concerns and concerns over cybercrimes such as electronic card fraud.[41] With respect to cybercrime, the CBN has observed an increase in number and sophistication of cybersecurity threats that target banks and electronic payment service platforms.[42] A report from the Nigerian Inter-Bank Settlement System (NIBSS) estimates that the banking sector lost over 12 billion Naira to various forms of cybercrime between 2014 and 2017.[43] Cybercrimes that target consumers in the Nigerian banking and financial sector include phishing, electronic card fraud, ATM scams, hacking of bank accounts and Business Email Compromise fraud.[44] It may not be possible to totally eradicate all cybercrime which target consumers that use banking and payment channels. However, the population of consumers using such channels for transactions would likely increase with improved consumer protection responses that enhances a high degree of consumer trust in the use of those channels.

2 The Development of Nigeria's Legal Response to Cybercrime

Prior to the widespread availability of internet access within Africa,[45] Nigeria gained global notoriety as a major source of a fraudulent activity known as 'advance fee fraud' or the *West African Letter Scam*.[46] This form of scam involves the act of obtaining property by false pretense[47] and appears similar to the *Spanish prisoner*

---

[34] *See* National Bureau of Statistics, *PoS Adoption and Usage: A Study on Lagos State* (National Bureau of Statistics 2015) 9.

[35] *Ibid.*

[36] *See* Central Bank of Nigeria (CBN) *Industry Policy on Retail Cash Collection and Lodgment (IITP/C/001)* Ref: COD/DIR/GEN/CIT/05/031 (20 April, 2011).

[37] *See* Uchenna Jerome Orji, 'Building a Cashless Economy in Nigeria: An Analysis of the Policy Framework and Proposals for Responses', 27(7) *Journal of International Banking Law and Regulation* (2012) 265–271.

[38] *See* National Bureau of Statistics, (n 34) 22.

[39] *See* Chuka Odittah, 'More Nigerians Used ATM Electronic Banking in 2016, says NBS Report', *The Guardian* (29 January, 2017) <https://www.guardian.ng/news/more-nigerians-used-atm-electronic-banking-in2016-says-nbs-report/>; National Bureau of Statistics, '2017 POS Analysis' (2017) <https://www.nibss-plc.com.ng/pos-statistics-2016/>; National Bureau of Statistics, '2016 POS Statistics', (2016) <https://www.nibss-plc.com.ng/pos-statistics-2016/> accessed 5 November, 2018.

[40] *See* National Bureau of Statistics, (n 34) 37.

[41] *Ibid* at 34.

[42] *See* Central Bank of Nigeria, *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers* (25 June, 2018) 1.

[43] *See* Editorial, 'Nigerian Banks Lose N12.30 Billion to Fraud in 4 Years- NIBSS', *The Vanguard* (21 June, 2018) <https://www.vanguardngr.com/2018/06/nigerian-banks-losen12–30bn-fraud-4-years-nibss/> accessed 5 November, 2018.

[44] *See* Osita Nwanu, 'E-Fraud in Nigeria: Growing or Dying Trend', in *Nigerian E-Fraud Forum 2015 Annual Report: Improving and Securing the Cyber Environment* (Central Bank of Nigeria 2015) 18–20; F. Wada and G.O. Odulaja, 'Electronic Banking and Cyber Crime in Nigeria – A Theoretical Policy Perspective on Causation', 4(3:2) *African Journal of Computing & ICT*, (2012) 71–75.

[45] Internet use data also indicate that Africa's Internet user population grew from 4,514,400 million people in 2000 to 453.3 million people in December, 2017, representing approximately 35.2 percent of Africa's entire population estimate. *See* Miniwatts Marketing Group, 'Internet Usage Statistics for Africa', (31 December, 2017) <https://www.internetworldstats.com/stats1.htm> accessed 5 November, 2018.

[46] The scam is also known as the 'Nigerian Letter Scam' or the '419 Scam' after Section 419 of the Nigerian Code.

[47] *See* Uchenna Jerome Orji, 'Curbing Advance Fee Fraud in Nigeria: An Analysis of the Regulatory Framework and Contemporary Challenges', 22(12) *International Company and Commercial Law Review*, (2011) 409; Andrews Atta-Asamoah, 'Understanding the West African Cybercrime Process', 18(4) *African Security Review* (2010) 106–114; Ben Simon Okolo, 'Demystifying the Advance fee Fraud Criminal Network', 18(7) *African Security Review* (2009) 11.

scam which originated in Europe during the 16th century.[48] In modern times, however, the origin of the scam has been erroneously linked to Nigeria and the West African region due to its seeming prevalence in those areas.[49] Nevertheless, there is no doubt that the increasing spread of information communication technologies and internet penetration within the West African region around the first decade of the 21st century also brought about the migration of advance fee fraud scammers to internet platforms, with Ghana and Nigeria being classified as major sources of internet advance fee fraud scams.[50] Thus, Nigeria's increasing internet penetration and telecommunications access also had implications on the rise of cybercrime perpetration in the country.[51]

The need to address cybercrime in Nigeria was first noted in the National Policy for Information Technology (2001), which recognized the importance of establishing appropriate laws to tackle computer crimes and protect online business transactions.[52] Later, in 2003, the Nigerian Government established the Presidential Committee on 419[53] Activities in the Cyberspace to propose legal and policy measures to tackle online advance fraud and other forms of cybercrime.[54] In 2004, the Nigerian Government also established the Nigerian Cybercrime Working Group (NCWG) after a 72-year-old internet scam victim from Czech Republic, who was allegedly defrauded by a Nigerian internet scammer, killed a diplomat at the Nigerian Embassy in Prague.[55] In 2005, the NCWG developed the Nigerian Computer Security and Critical Information Infrastructure Protection Bill. The Bill marked the first attempt to establish a cybercrime law in Nigeria, and also sought to establish a legal framework for cybersecurity and the protection of critical information infrastructure. However, the Bill did not receive meaningful attention in the Nigeria National Legislative Assembly and was therefore never passed into law.[56]

In 2006, Nigeria enacted the Advance Fee Fraud Act[57] to tackle advance fee fraud activities in Nigeria. The language of the Act is couched in a manner that criminalizes advance fee fraud activities regardless of whether such activities were perpetrated in a physical environment, or on the internet. The Act also criminalizes activities that constitute advance fee fraud where there is intent to defraud persons in Nigeria, or any other country.[58] Offences under the Act include the act of obtaining property by false pretense,[59] and the laundering of funds obtained through advance fee fraud activities.[60] In order to prevent the use of internet and telecommunication facilities and services for the purpose of perpetrating advance fee fraud, the Act requires telecommunication service providers and internet service providers as well as the proprietors of telephone and internet cafes to identify their subscribers and customers[61] and register their business with the EFCC.[62] The Act also requires the above businesses to exercise a "duty of care" by ensuring that their services and facilities are not utilized for the perpetration of advance fee fraud scams.[63] However, while the Act criminalized advance fee fraud scams such as email scams, it did not criminalize other forms of

[48] *See* Keiran Dunne, 'Nigerian 419 E-Mail Scams', *The ATA Chronicle* (July, 2007) 33; Harvey Glickman, 'The Nigeria '419' Advance Fee Scams: Prank or Peril?', 39(3) *Canadian Journal of Africa Studies* (2005) 472; Russell G. Smith, Michael N. Holmes and Philip Kaufmann, 'Nigerian Advance Fee Fraud', (121)1 *Trends and Issues in Crime and Criminal Justice* (1991).

[49] *See* Caroline Baylon and Albert Antwi-Boasiako, *Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study* (Centre for International Governance Innovation and Chatham House, 2016) 6; Ultra Advanced Global Investigations, *419 Advance Fee Fraud Statistics 2009* (Amsterdam, 2010) 13. For further discussion *see* Orji, (n 47) 408–409.

[50] *See* Internet Crime Complaint Center, *2010 Internet Crime Report* (National White Collar Crime Center 2011) 11; Internet Crime Complaint Center, *2013 Internet Crime Report* (National White Collar Crime Center 2014) 15 and 21.

[51] *See* Orji, (n 47) 408–421.

[52] *See* Nigerian National Policy for Information Technology, (2001) 3 and 28.

[53] The acronym '419' is derived from the provisions of section 419 of the Nigerian Criminal Code which was the first Nigerian law to criminalize the act of obtaining money or property by false pretense. *See* Nigerian Criminal Code Act, Chapter 77, Laws of the Federation of Nigeria (1990) s 419.

[54] S*ee* Orji, (n 9) 497.

[55] *See* BBC News, 'Diplomat shot Dead in Prague', *BBC News* (19 February, 2003) <http://news.bbc.co.uk/2/hi/Europe/2780259.stm>; John Leyden, 'World's First 419 Revenge Killing?: Czech Police Hold Man after Nigerian Embassy Shooting, *The Register* (20 February, 2003) <https://www.theregister.co.uk/2003/02/20/worlds_first_419_revenge_killing/> accessed 5 November, 2018.

[56] For an analysis of the Bill, *see* Orji, (n 9) 508–533.

[57] *See* The Nigerian Advance Fee Fraud and Other Related Offences Act 2006.

[58] *See* Orji, (n 47) 409–410.

[59] *See* Advance Fee Fraud Act 2006, s 1.

[60] *See* Advance Fee Fraud Act 2006, s 7.

[61] *See* Advance Fee Fraud Act 2006, s 12.

[62] *See* Advance Fee Fraud Act 2006, s 13(1) (a).

[63] *See* Advance Fee Fraud Act 2006, s 13(3).

cybercrime that could affect consumers of electronic banking and payment services such as unauthorized access, system interference, phishing, card fraud and ATM scams.

Later, in 2009, the Nigerian Cybersecurity and Data Protection Bill was introduced in the House of Representatives. The Bill sought to criminalize cybercrime and establish a Cybersecurity and Information Protection Agency that would be responsible for the protection of computer systems and networks.[64] However, the Bill did not pass in the House of Representatives. In 2011, a new cybersecurity Bill was introduced as an Executive Bill in the National Assembly. In that same year, the House of Representatives proposed amendments to the Nigerian Criminal Code to address computer misuse and cybercrime. Both Bills could not succeed due to lack of legislative attention. The Nigerian Federal Ministry of Justice also opposed the proposed amendments to the Criminal Code and advised that a comprehensive Executive Bill on cybercrimes would be a better approach than amending the Criminal and Penal Codes.[65] On 18 December, 2013, a new Bill titled the Nigerian Cybercrimes Bill (2013) was also introduced in the National Assembly as an Executive Bill of the President the Federal Republic of Nigeria. This Bill was later enacted in 2015 as the Cybercrimes (Prohibition and Prevention) Act.[66] The Act seeks to provide a comprehensive and effective legal and regulatory framework for the prohibition, prevention, detection and prosecution of cybercrime in Nigeria.[67] It also provides for the protection of computer systems and networks as well as critical information national infrastructure.[68]

The Nigerian Cybercrimes Act applies if a cybercrime victim is located in Nigeria, or resident in Nigeria or on a ship or aircraft registered in Nigeria.[69] This implies that with respect to cybercrime that target electronic banking and payment channels, the Act would apply in situations where the affected consumer is in Nigeria, or resident in Nigeria or was using electronic banking and payment channels on board a ship or aircraft registered in Nigeria. The Act also appears to have an extraterritorial jurisdictional scope. In this regard, the Act applies outside Nigeria if an affected consumer is a citizen or resident of Nigeria.[70] Thus, the Act implicitly enshrines the concept of a 'significant link'[71] with Nigeria so that Nigerian courts can exercise extraterritorial jurisdiction over cybercrime offences which affect a Nigerian citizen or resident that consumes electronic banking services. The concept of a 'significant link' has been applied in several other jurisdictions so as to enable courts to assume jurisdiction over cybercrime offences once there is a link between the offence or offender and the country claiming jurisdiction.[72] The need for enshrining the significant link concept in cybercrime laws appears to arise from the cross-border interconnection of information and communication networks, which makes it impossible to confine such networks within national borders, and therefore creates a real possibility that computer systems and individuals within a particular country can be affected by malicious acts from criminal actors located in other countries.[73]

The Act also applies to acts committed outside Nigeria where an offender who has allegedly committed a cybercrime that is prohibited under Act is located in Nigeria and is not extradited to another country for prosecution.[74] As such, the Act appears to technically enshrine the doctrine of *aut dedere aut judicare* (extradite or prosecute).[75] This makes it easier to hold offenders accountable where they commit cybercrime offences in other countries and flee to Nigeria. Therefore, the Act makes it difficult for Nigeria to be used as a safe haven by offenders who engage in forum shopping so as to technically evade prosecution or extradition for cybercrime offences.[76]

---

[64] *See* The Nigerian Cybersecurity and Data Protection Agency Bill – HB, 154, C4443, 2008. For an analysis of the Bill, *see* Orji, (n 9) 535–537.

[65] *See* Abikoye Oluwafemi and Yusuf Salibu 'Cybersecurity in Nigeria: Need for a Paradigm Shift', (3)1 *Paradigm Initiative Policy Brief* (3 July, 2014).

[66] *See* The Cybercrimes (Prohibition and Prevention etc) Act 2015.

[67] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 1.

[68] *Ibid.*

[69] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 50 (1) (a)–(c).

[70] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 50 (1) (d)–(i).

[71] S*ee* Orji, (n 9) 252.

[72] *Ibid* at 220, 252, and 280.

[73] *See* Uchenna Jerome Orji, 'Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States', 6(1) *Defence Against Terrorism Review* (2014) 31–32; Uchenna Jerome Orji, *International Telecommunications Law and Policy* (Cambridge Scholars Publishing 2018) 1.

[74] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 50 (1) (d)–(ii).

[75] *See* Bryan A. Garner (ed), *The Black's Law Dictionary* (9th edn, West Publishing Co 2009) 151.

[76] *See* Uchenna Jerome Orji, 'Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation?', in Markus Maybaum, *et al* (eds), *Architectures in Cyberspace- 7th International Conference on Cyber Conflict* (NATO CCD COE 2015) 111–112.

3 An Analytical Overview of the Consumer Protection Regime under the Cybercrimes Act

The Nigerian Cybercrimes Act generally criminalizes several forms of cybercrime that affect the banking and financial sector. For example, the Act criminalizes computer related forgery;[77] computer related fraud; [78] the transmission of electronic mails with intent to defraud;[79] unlawful diversion of banking and financial electronic mails with intent to defraud;[80] unauthorized modification of computer data;[81] unauthorized hindering of computer systems;[82] insider collusion to perpetrate fraud on bank customers;[83] and, the theft of payment terminals or electronic devices such as ATM and PoS terminals.[84] In addition to the above, the Act establishes specific provisions that aim to protect consumers of banking and financial services. Those specific provisions will be discussed below.

3.1 Duty of Banks and Financial Institutions to Establish Effective Measures to Prevent Cybercrime

Banks and financial institutions occupy the most strategic position in the electronic banking and payment services system. This is because banks and financial institutions supply electronic banking and payment services to consumers which require them to acquire and hold sensitive confidential information that relate to consumers on their computer systems, such as bank account details and transaction records. More importantly however, the contractual relationship between banking and financial institutions and the consumers of their services includes an implied fiduciary duty of secrecy and confidentiality.[85] This means that a bank or financial institution is under an implied obligation to protect the confidentiality of a customer's account details and transactions made thereon.[86] Therefore, banks and financial institutions, given their stronger position in relationship with consumers, generally have a duty to adequately protect the confidential information of consumers that use their services from unauthorized access by third parties. Accordingly, Section 19(3) of the Cybercrimes Act provides that:

> "Financial institutions must as a duty to their customers put in place effective counter fraud measures to safeguard their sensitive information, *where a security breach occurs the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity*".[87]

The above provision requires banks and financial institutions to establish effective fraud prevention measures to protect the 'sensitive information' of customers held in their computer systems from being unlawfully accessed by unauthorized third parties. The Act does not define the meaning of 'sensitive information' and such definition does not exist under relevant banking laws in Nigeria. However, the CBN Consumer Protection Framework of 2016, which Nigerian banks and financial institutions are required to comply with,[88] appears to provide an industry working classification of what can be regarded as 'sensitive information'. In this regard, the CBN Consumer Protection Framework, provides that "the following information are considered to be confidential and shall be protected at all times; contact details, account number and

---

[77] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 13.

[78] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 14(1).

[79] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 14(4).

[80] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 14(4) (a).

[81] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 16(1).

[82] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 16(3).

[83] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 14(5)

[84] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 15.

[85] *See* Uchenna Jerome Orji, 'A Review of the Special Duties of Banks under the Nigerian Money Laundering Act', *Journal of International Banking Law and Regulation* (2011) 26 (6)305.

[86] *See* for e.g., the English case of *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 46, where the Court held that the relationship between a customer and banker is a confidential one, and stated that it is an implied term of contract between a banker and the customer that the banker will not divulge to third parties either the state of the customer's account or any of his or her transactions with the bank or any information relating to the customer which was acquired through the keeping of his or her account.

[87] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 19(3). (Emphasis added).

[88] The CBN Consumer Protection Framework of 2016 was established in the exercise of the CBN's powers to issue regulatory guidelines for the purpose of governing the operation of banks and financial institutions in Nigeria. Compliance with CBN regulatory guidelines such as the Consumer Protection Framework is mandatory for banks and financial institutions in Nigeria and non-compliance can result in regulatory sanctions including fines and the revocation of operational licenses. *See* Banks and Other Financial Institutions Act, 1991 (As Amended), s 60 (2), (4) and 64. *See* Central Bank of Nigeria Act, 2007, s 33(1) (b) and 33 (5).

balance, statement of accounts and any other information known to the financial institution".[89] Thus, within the context of section 19(3) of the Cybercrimes Act, 'sensitive information' will include personal banking details such as an account name, account number and personal identification numbers or codes which can be used to access a customer's account to perpetrate fraud, as well as any information about a consumer that has been acquired by a bank or financial institution.

To a large extent under section 19(3) of the Cybercrimes Act, where a security breach occurs, the proof of negligence will lie on the customer who has to prove that the bank or financial institution could have done more to safeguard his or her information. It is submitted this requirement appears to defeat the consumer protection objective of section 19(3). This is because the section does not put the bank or financial institution, which is the stronger party in the contractual relationship with the consumer, in a position where it will bear greater liability for the breach of consumer data held in its computer system. Rather, the section places consumers in a difficult position whereby they will always have to prove that their banks or financial institutions were negligent in all situations where their sensitive data was accessed by unauthorized third parties. In addition, the requirement also weakens the implied fiduciary obligation of secrecy and confidentiality that banks and financial institutions owe the consumers of their services to safeguard their information. Therefore, the provision enshrines a weak liability regime which appears to reduce regulatory incentive for banks and financial institutions that supply electronic banking and payment services to develop effective measures for safeguarding the sensitive personal data of consumers held or processed on their computer systems. The absence of such strong regulatory incentive can however produce the undesirable effect of reducing consumer trust in electronic banking and payment transactions. The challenge presented by the weak liability regime under section 19(3) of the Act is also compounded by the fact that Nigeria has not enacted a data protection law to protect the sensitive personal data of individuals,[90] including consumers that use electronic banking and payment services. Furthermore, consumers may lack the requisite information and technical capability to conveniently prove that banks or financial institutions were negligent in safeguarding their data. Also, while the CBN Consumer Protection Framework imposes a duty of care on banks and financial institutions to safeguard the privacy of all personal information of customers including those with closed accounts,[91] the Framework does not address the proof of negligence where a security breach has affected customer's information that is held by a bank or financial institution.

However, imposing a greater or strict liability regime on banks and financial institutions under section 19(3) of the Cybercrimes Act will make them have a higher degree of liability for the breach of consumer data and also encourage them to develop better security measures to prevent cybercrime including fraud. Such a higher liability approach has been adopted as a governing principle under the European Union (EU) Directive on Payment Services in the Internal Market which requires that:

> "Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations …it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases".[92]

In the Nigerian context, it is submitted that an amendment of section 19(3) of the Cybercrimes Act to adopt an approach that is similar to the EU Directive on Payment Services will have the effect of increasing the protection of consumers of electronic banking and payment services from cybercrime. In particular, adopting such an approach will reduce the high burden of proof on a consumer to prove that the breach of the security of his or her data held by a bank or financial institution resulted from the negligence of such bank and financial institution to adequately protect such data. An amendment that will reduce the high burden of proof on a consumer under section 19(3) also appears necessary because a consumer has very limited information about the security architecture of computer systems of a bank or financial institution that holds or processes his or her data. This will therefore make it difficult if not impossible for a consumer to technically discharge the burden of proof under section 19(3) in order to successfully prove that a bank or

---

[89] *See* Central Bank of Nigeria, *Consumer Protection Framework* (7 November, 2016) at 21, para 2.6.

[90] *See* Uchenna Jerome Orji, 'Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act', *International Data Privacy Law* (2017) 7 (3)186–187.

[91] *See* Central Bank of Nigeria, *Consumer Protection Framework* (7 November, 2016) at 23, para 2.6.2.

[92] *See* European Union Directive 2015/2366 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (November, 2015) at para 72. [Hereafter, EU Directive on Payment Services].

financial institution was negligent in safeguarding his or her data from unauthorized access. Therefore, an amendment that will reduce the high burden of proof on consumers will also go a long way towards enhancing the accountability of banks and financial institutions for the security of consumers' data held in their computer systems.

3.2 Issuing Unlawful Electronic Banking Instructions

Section 20 of the Cybercrimes Act provides that:

> "Any person being authorized by any financial institution and charged with the responsibility of using computer or other electronic devices for financial transactions such as posting of debit and credit, issuance of electronic instructions as they relate to sending of electronic debit and credit messages or charged with the duty of confirmation of electronic fund transfer, unlawfully with the intent to defraud issues false electronic or verbal messages is guilty of an offence and is liable to imprisonment for 7 years".[93]

The above provision prohibits the unlawful issuance of an electronic banking instruction by the staff of a bank or financial institution where there is an intent to defraud. The section does not prescribe that the intent to defraud will have to be targeted at either a consumer or banking/financial institution for criminal liability to attach, and therefore it applies to instances where a consumer is the target. Such instances include where a customer's account has been debited without authorization by the staff of a bank or financial institution with the intent of defrauding the customer. Thus, the provision recognizes that insiders such as employees of banks and financial institutions can engage in cybercrime that may include the unauthorized issuance of electronic banking or payment instructions with the intent of defrauding customers and therefore it aims to criminalize such acts by insiders within a bank or financial institution.

3.3 Unlawfully Obtaining the Identity of a Bank or Financial Institution with Intent to Defraud

Section 22(1) of the Cybercrimes Act provides that:

> "Any person who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft of its employer, staff, service providers and consultants with the intent to defraud is guilty of an offence and upon conviction shall be sentenced to 7 years imprisonment or N5,000,000.00 fine or both".[94]

The above provision criminalizes the theft of a bank or financial institution's identity by an insider such as an employee with the intent of using such identity for fraudulent purposes. Within context, the section does not prescribe that the intent to defraud will have to be targeted at either a consumer or banking/financial institution for criminal liability to attach, as such, the provision would also cover situations where the staff of a bank or financial institution has unlawfully used its identity or the identity of its employees or consultants to defraud a customer. For example, an employee of a bank that directs a customer to a fake bank website that appears similar to the genuine one, with the intent of defrauding such customer will be liable under section 22(1) of the Cybercrimes Act.

3.4 Unlawful Disclosure of a Password or Access Code

Section 28(3) of the Cybercrimes Act provides that:

> "Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer or network for any unlawful purpose or gain, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both fine and imprisonment".[95]

---

[93] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 20.

[94] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 20.

[95] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 28(3).

The above provision criminalizes unauthorized disclosure of passwords or access codes for the purpose of accessing any program or data held in any computer or network where the intent of such disclosure is to facilitate any unlawful act or make an unlawful gain. Thus, once there is an intent of furthering an unlawful act or making an unlawful gain, the provision would cover a situation where a person has unlawfully disclosed any password or access code that can be used to gain access to a consumer's personal banking details or data held on a bank's computer or network. For example, in Nigeria, bank customers are required to physically visit their banks to collect their electronic bank cards such as ATM cards as well as the Personal Identity Numbers (PINs) of such cards. Customers are usually advised by their banks to immediately change the PIN originally assigned to such cards before making transactions. In some cases, customers may forget to change such PINs or may sometimes lack the skill to change them, this then exposes their accounts to cybercrime if such PINs are disclosed to cyber criminals by bank employees who are aware of them, however, section 28(3) of the Cybercrimes Act broadly criminalizes such act and protects consumers by prohibiting the unlawful disclosure of their passwords or access codes by any person including bank employees. In addition, the Cybercrimes Act also criminalizes the unauthorized use of a password or access code including electronic signature or other unique identification belonging to another person.[96]

3.5 Unlawful Use of a Consumer's Security Code by a Service Provider or Vendor of Computer Based Services

Section 29(1) of the Cybercrimes Act provides that:

> "Any person or organization who being a computer based service provider and or vendor does any act with intent to defraud and by virtue of his position as a service provider, forges, illegally uses security codes of the consumer with the intent to gain any financial and or material advantage or with intent to provide less value for money in his or its services to the consumer shall if corporate organization be guilty of an offence and is liable to a fine of N5,000,000.00 and forfeiture of further equivalent of the monetary value of the loss sustained by the consumer".[97]

The above section aims to promote consumer protection by prohibiting a service provider or vendor of computer based services (such as electronic banking or payment services) from unlawfully using or forging a consumer's security code with the intent of defrauding the consumer, or obtaining financial or material gain, or providing less service against the value of money paid by the consumer. For example, the provision will apply where a service provider or vendor of electronic banking or payment services, unlawfully uses or forges a consumer's security code to make unauthorized withdrawals from the consumer's bank account.

3.6 Unlawful Manipulation of ATM Machines and PoS Terminals

Section 30(1) of the Cybercrimes Act provides that:

> "Any person who manipulates an ATM machine or Point of Sales (PoS) terminals with the intention to defraud shall be guilty of an offence and upon conviction sentenced to Five Years imprisonment or N5,000,000.00 fine or both".[98]

Section 30(2) of the Act also provides that:

> "Any employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using an ATM of PoS device, shall be guilty of an offence and upon conviction sentenced to Seven Years imprisonment without an option of fine".[99]

The above provisions of sections 30(1) and (2) criminalize the manipulation of ATM machines and PoS terminals with intent to defraud and also prohibits the commission or facilitation of such act by insiders such as the employees of banks and financial institutions. The section does not prescribe that the intent to defraud will have to be targeted at either a consumer or banking/financial institution for criminal liability to attach.

---

[96] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 22(2).

[97] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 29(1).

[98] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 30 (1).

[99] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 30 (2).

Therefore, the provision applies to situations where an ATM machine or PoS terminal has been manipulated for the purpose of defrauding a customer. Thus, to a large extent, the provision promotes the protection of the customers of banks or financial institutions that use ATM machine and PoS terminals for electronic banking or payment transactions, and therefore it enhances consumer trust in the use of such electronic banking and payment channels.

3.7 Phishing Scams and Electronic Card Fraud

The Cybercrimes Act criminalizes phishing scams that target consumers in the banking and financial sector. In this regard, section 32(1) of the Act provides that "any person who knowingly or intentionally engages in computer phishing shall be liable upon conviction to 3 years imprisonment or a fine of N1,000,000.00 or both".[100] Section 58 of the Cybercrimes Act defines 'phishing' as "the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and Credit card details, by masquerading as a trustworthy entity in an electronic communication through e-mails or instant messaging either in form of an email from what appears from a bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user".[101] By prohibiting phishing the Act promotes the protection of consumers who use electronic banking and payment platforms because phishing scams are usually deployed by cyber criminals to obtain confidential information that can be used to unlawfully access a consumer's account for fraudulent purposes.[102]

The Cybercrimes Act also aims to protect consumers who use electronic cards on electronic banking and payment platforms by prohibiting fraudulent activities that target cards used on such platforms. For example, section 33(1) of the Act criminalizes the use of electronic cards (including credit cards, debit cards and other forms of electronic cards) to fraudulently obtain cash, credit, goods, or service.[103] In addition, the Act criminalizes the theft of an electronic card, and a person convicted of such offence would be required to repay the cardholder the value of loss sustained as a result of the theft.[104] The Act also criminalizes the intentional receipt, use, sale or traffic of lost electronic cards.[105] Other acts that are criminalized with respect to electronic cards include the use of forged or fraudulently obtained electronic cards in financial transactions,[106] the manufacture of counterfeit electronic cards,[107] the disclosure of a cardholder's account number and address to a third party without the consent of the cardholder,[108] and the acquisition of a cardholder's confidential details for fraudulent purposes.[109]

3.8 Duty of Banks and Financial Institutions to Report Cyber Threats

Section 21(1) of the Cybercrimes Act imposes obligations on persons or institutions that operate a computer network to report cyber threats. It provides that:

> "Any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team (CERT) Coordination Center of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues".[110]

Thus, section 21(1) of the Cybercrimes Act imposes a duty on organizations including banks and financial institutions that operate computer systems and networks to report the occurrence of any cyber threats such as unlawful attacks and intrusions that affect consumer data held on their computer systems and networks to Nigeria's National CERT Coordination Center. In addition, the CBN's Risk-based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers which Nigerian banks and financial institutions are required to comply with, also imposes a similar reporting obligation on banks and

[100] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 58.
[101] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 32(1).
[102] S*ee* Orji, (n 9) 40.
[103] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 33(1).
[104] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 33(3).
[105] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 33(4) and 34.
[106] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 33(5)–(9).
[107] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 33(10).
[108] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 33(12).
[109] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 36(1).
[110] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 21(1).

electronic payment service providers by requiring them "to report all cyber-incidents whether successful or not immediately after such incident was identified to the Director of Banking Supervision of the CBN".[111] A major aim of the cyber threat reporting obligation is to facilitate a timely national response to cyber incidents that may affect data held on the computer systems and networks of organizations, including banks and financial institutions that provide electronic banking and payment services. For example, confidential information relating to the bank accounts of consumers that use electronic banking and payment services, which is being held on the computer network of a bank, may be breached as a result of an intrusion into the bank's network. However, the reporting obligation seeks to ensure that such breaches are properly addressed once they are identified so as limit their escalation across the entire banking and financial sector. As such, the requirement promotes the protection of sensitive consumer data in the sector and also has the effect of improving network resilience and consumer confidence in the use of electronic banking and payment services.

3.9 Duty of Banks and Financial Institutions to Verify Customer Identity before Executing Electronic Banking Transactions

Section 37(1) of the Cybercrimes Act imposes obligations on banks and financial institutions to verify the identity of a customer before carrying out electronic banking transactions. It provides that:

> "A financial institution shall verify the identity of its customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before issuance of ATM cards, credit cards, debit cards and other related electronic devices".[112]

The above provision requires banks and financial institutions to properly identify their customers before issuing them with ATM cards, credit cards, debit cards and other related electronic devices. In practice, the identification of a customer by a bank and financial institution in Nigeria will include the acquisition of the customer's personal data and biometric details, and the issuance or confirmation of the Bank Verification Number which was introduced by the CBN to create an accurate database of bank customers.[113] The proper identification of customers by banking and financial institutions is a crucial element of any banking and financial transaction and usually is a prerequisite for any form of business relationship between a bank and a customer to occur. This duty is commonly known as the "Know Your Customer" (KYC) principle. Generally, the purpose of customer identification is to ensure that a bank or financial institution does not engage in transactions with a customer, unless it is aware of the customer's identity.[114] The KYC requirement under section 37(1) of the Cybercrimes Act has the effect of enhancing consumer protection in the use of electronic banking and payment platforms because it aims to ensure that stolen identification is not used to fraudulently access a consumer's account. In addition, the KYC requirement helps to ensure that the perpetrators of fraudulent electronic banking and payment activities are traced and held accountable. This also helps to discourage the perpetration of fraud against consumers that use electronic banking and payment services.

3.10 Duty of Banks and Financial Institutions to Reverse Unauthorized Withdrawals

Section 37(3) of the Cybercrimes Act imposes a duty on banks and financial institutions to reverse an unauthorized withdrawal from the account of a customer. It provides that:

> "Any financial institution that makes an unauthorized debit on a customer's account shall upon written notification by the customer, provide clear legal authorization for such debit to the customer or reverse such debit within 72 hours. Any financial institution that fails to reverse such debit within 72 hours, shall be guilty of an offence and liable on conviction to restitution of the debit and a fine of N5, 000,000.00".[115]

---

[111] *See* Central Bank of Nigeria, *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers* (25 June, 2018) 10 at para 7.6.

[112] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 37(1).

[113] *See* Central Bank of Nigeria, *Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry*, BPS/DIR/GEN/CIR/04/010 (18 October, 2017).

[114] *See* Uchenna Jerome Orji, 'A Review of the Special Duties of Banks under the Nigerian Money Laundering Act', *Journal of International Banking Law and Regulation* (2011) 26 (6) 301.

[115] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 37(1).

The above provision requires a bank or financial institution that has made an unauthorized debit on a customer's account to provide clear legal authorization for such debit upon a written notification by the customer, or reverse such debit within 72 hours. The provision aims to protect bank customers that use electronic cards on electronic banking and payment platforms from being debited in error due to issues including fraud and the malfunction of payment devices such as ATM and PoS terminals. Apparently, the provision became necessary to address reoccurring cases of unauthorized account debits arising from fraud and the malfunction of ATM terminals in the Nigerian banking industry. For example, there are instances where card users may operate ATMs to withdraw money without success and their accounts are debited in error although they had not obtained money from the machine. There are also instances where a card user may request to withdraw a particular sum of money from the ATM, only for the machine to dispense a lower amount and erroneously debit the card user's account to the full amount.[116] In most cases, a card user whose account has been wrongly debited while using an ATM is faced with the challenge of resolving the issue with the bank and retrieving the debited funds. To address this state of affairs, the Central Bank of Nigeria issued a consumer protection directive in 2010 which required all Nigerian banks to handle all consumer complaints on ATM transactions within 72 hours of receiving such complaint.[117] Thus, section 37(3) of the Cybercrimes Act appears to have enshrined that CBN consumer protection directive as part of Nigerian law.

However, the Cybercrimes Act does not establish a regime for determining when card users or their banks/financial institutions are liable for unauthorized debits arising from fraud. For example, the Act does not explicitly address the level of a card user's liability for unauthorized debits on his or her account which arises from a cybercrime due to negligence on the part of the card user or his or her bank or financial institution.

To some extent, the CBN Consumer Protection Framework attempts to address a card user's liability for unauthorized debits on his or her account arising from negligence. The Framework provides that "financial institutions shall promptly refund customers for actual amounts lost due to fraud with interest at the CBN prescribed rate *unless it can be proved that loss occurred as a result of customer's negligence or through fraudulent behavior*".[118] The CBN Guidelines on Operations of Electronic Payment Channels in Nigeria (2016) also attempts to address the liability of a card holder for unauthorized account debits which arise from negligence by providing that "the cardholder shall be held liable for fraud committed with his card, arising from the misuse of his PIN or his card".[119] A similar provision exists under the CBN Guidelines on Electronic Banking (2003) which provides that "...the cardholder will be liable for frauds arising from PIN misuse".[120] However, the CBN's regulatory instruments (the CBN Consumer Protection Framework, the Guidelines on Operations of Electronic Payment Channels, and the Guidelines on Electronic Banking) just like the Cybercrimes Act, do not adequately address a card user's liability for unauthorized debits which have occurred as a result of a cybercrime arising from negligence on the part of the card user or a bank or financial institution. For example, there are no provisions on the degree of a bank or financial institution's liability where a customer has reported that his or her electronic bank card or other confidential electronic banking or payment details has been compromised as a result of negligence or other factors such as duress or theft. In such circumstances, would the customer still be liable for any unauthorized debits that take place after he or she has made a report to the relevant bank or financial institution? It is submitted that this possible scenario has not been addressed in the Cybercrimes Act or under the CBN's Consumer Protection Framework and the Guidelines on Operations of Electronic Payment Channels. Therefore, it appears necessary to consider responses in other parts of the world.

3.10.1 Lessons from other Jurisdictions

Banking legislations in some other parts of the world have tried to prescribe an explicit liability regime to address unauthorized debits to the accounts of card users due to negligence on the part of the card user or his or her bank or financial institution. In the United States, for example, the Electronic Funds Transfer Act

---

[116] *See* Editorial, 'Nigeria's ATM Galleries of Failure', *Leadership* (23 July, 2017) <https://www.leadership.ng/2017/07/23/nigerias-atm-galleries-failure>; Oyetunji Abioye, 'Resolving ATM Cash Dispense Error with Ease', *Punch* (26 October, 2016) <https://www.punchng.com/resolving-atm-cash-dispense-error-ease> accessed 5 November, 2018.

[117] *See* Uchenna Jerome Orji, 'Creating a Sustainable Legal and Regulatory Environment for Electronic Banking in Nigeria', *Journal of International Banking Law and Regulation* (2011) 26 (12) 614.

[118] *See* Central Bank of Nigeria, *Consumer Protection Framework* (7 November, 2016) at 23 para 2.6.1.5. (Emphasis added).

[119] *See* Central Bank of Nigeria, *Guidelines on Operations of Electronic Payment Channels in Nigeria* (April, 2016), at 17 and 28 paras, 2.4.6.5 and 3.4.6.5.

[120] *See* Central Bank of Nigeria, *Guidelines on Electronic Banking in Nigeria* (August, 2003) at 3 para 1.4.2.

(EFTA) provides for the protection of consumer rights in electronic banking and funds transfer systems.[121] In particular, the EFTA establishes explicit provisions for consumer liability in the event of an unauthorized electronic fund transfer.[122] The Act provides that:

> "A consumer shall be liable for any unauthorized electronic fund transfer involving the account of such consumer only if the card or other means of access utilized for such transfer was an accepted card or other means of access and if the issuer of such card, code, or other means of access has provided a means whereby the user of such card, code, or other means of access can be identified as the person authorized to use it, such as by signature, photograph, or fingerprint or by electronic or mechanical confirmation. In no event, however, shall a consumer's liability for an unauthorized transfer exceed the lesser of—
>
> (1) $50; or,
>
> (2) the amount of money or value of property or services obtained in such unauthorized electronic fund transfer prior to the time the financial institution is notified of, or otherwise becomes aware of, circumstances which lead to the reasonable belief that an unauthorized electronic fund transfer involving the consumer's account has been or may be effected...".[123]

The above section clearly defines the limits of a consumer's liability in the event of an unauthorized funds transfer. It implies that for a consumer to be liable for an unauthorized electronic funds transfer from his or her account the following elements must exist:

1. firstly, the card or means of access utilized for such transfer must have been an 'accepted card' or 'other means of access';[124]
2. secondly, the issuer of the card must have provided a means whereby the user of such card can be identified as the person authorized to use it.[125]

However, where a consumer is liable for unauthorized transfer, such liability will not exceed 50 US dollars[126] or the amount of money obtained in the unauthorized transfer prior to notifying the financial institution that an unauthorized electronic fund transfer has been or may be made on the consumer's account.[127] Thus, a consumer is not liable for any further unauthorized transfers once a financial institution has been notified. A financial institution will however not be liable where a consumer fails to do so,[128] in such cases the consumer who fails to notify the financial institution of an unauthorized transfer as required by the Act will be liable instead.[129] Furthermore, a consumer's liability for an unauthorized transfer under the EFTA cannot be increased under other applicable laws or under any agreement with the consumer's financial institution.[130]

---

[121] *See* The Electronic Funds Transfer Act, United States Code: Title 15: section 1693 (a).

[122] *See* The Electronic Funds Transfer Act, United States Code: Title 15: section 1693(g).

[123] *See* The Electronic Funds Transfer Act, United States Code: Title 15: section 1693g (a). *See also* section 1693g (e) *ibid.*

[124] The term 'accepted card' or 'other means of access' is defined under the EFTA to mean a card, code, or other means of access to a consumer's account for the purpose of initiating electronic fund transfers when the person to whom such card or other means of access was issued has requested and received or has signed or has used, or authorized another to use, such card or other means of access for the purpose of transferring money between accounts or obtaining money, property, labor, or services. *See* The Electronic Funds Transfer Act, United States Code: Title 15: section 1693a(1).

[125] *See* The Electronic Funds Transfer Act, United States Code: Title 15: section 1693(g) (a).

[126] *Ibid.*

[127] *Ibid.*

[128] *See* Benjamin Geva, 'Payment Transactions Under the EU Payment Services Directive: A U.S. Comparative Perspective', *Penn State International Law Review* (2009) 27(3/4)732.

[129] *See, Krusser v Bank of America* (Cal Rpts. 463, CIV.ct.App.1994). In that case, a cardholder who believed that his debit card had been destroyed in 1986 failed to notify his bank of a 20 US dollar unauthorized ATM withdrawal which appeared in his bank statement in December, 1986. Later in September 1987, the cardholder received bank statements for July and August 1987, which indicated 47 unauthorized ATM withdrawals with the card, amounting to 9,020 US dollars. The cardholder then notified the bank of all unauthorized withdrawals including that which had earlier appeared in the bank statement of December 1986. The Court held that the cardholder's failure to report the unauthorized 20 dollar withdrawal, which appeared on December 1986 statement, barred him from recovering the loss incurred in July and August 1987. *See*, Benjamin Geva, *The Law of Electronic Funds Transfer*, (Lexis Publishing 2000) 105. *See also*, Kethi D. Kilonzo, 'An Analysis of the Legal Challenges posed by Electronic Banking', *Kenya Law Review* (2007) (1) 338–339.

[130] *See* The Electronic Funds Transfer Act, United States Code: Title 15: section 1693g (d).

In any case, such a law or agreement will be void to the extent of its inconsistency with the EFTA, unless the law purports to increase the rights of consumers and the liabilities of financial institutions.[131]

In the Europe Union, the Directive on Payment Services in the Internal Market establishes provisions that explicitly address a card user's liability for unauthorized debits on his or her account due to negligence on the part of the card user or his or her bank or financial institution. In this respect, the Directive requires Member States to "ensure that a payment transaction is considered to be authorized only if the payer has given consent to execute the payment transaction".[132] Thus, in the absence of consent, a payment transaction is considered to be unauthorized.[133] This implies that a card user will not be liable for any unauthorized debit on his or her account where the consumer did not authorize such transaction. The Directive also requires a payment service provider such as a bank that has been notified by a card user of an unauthorized or incorrectly executed payment transaction to rectify such transaction.[134] In addition, the Directive requires Member States to ensure that in the event of an unauthorized payment transaction, the payment service provider would restore the account of the affected consumer to its state prior to the unauthorized payment transaction, except where the payment service provider has reasonable grounds for suspecting fraud and files a formal report with the relevant national authority.[135]

More importantly, Article 74(1) of the Directive provides that the consumer "may be obliged to bear the losses relating to any unauthorized payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument".[136] This implies that a card user's liability for unauthorized payment transactions in case the card is lost or stolen or misappropriated is limited to EUR 50. The liability regime under Article 74(1) of the Directive will however not apply where the loss, theft or misappropriation of a payment instrument was not detectable to the consumer prior to a payment, except where the consumer has acted fraudulently;[137] or where the loss was caused by an employee, agent or branch of a payment service provider.[138] However, a consumer will be liable to bear all of the losses relating to any unauthorized payment transaction if they were incurred by the consumer acting fraudulently, or where the consumer intentionally fails to fulfill one or more of the obligations set out in Article 69 of the Directive or where there is gross negligence.[139] Under Article 69, a consumer using a payment service is required to use the service in accordance with the terms governing its use[140] and also take all reasonable steps to keep its personalized security credentials safe.[141] In addition, a consumer using a payment service is required to notify the payment service provider "without undue delay" on becoming aware of the loss, theft, misappropriation or unauthorized use of the payment instrument.[142] Also, one of operating principles of the Directive declares that a consumer should not be liable for all the losses relating to any unauthorized payment transaction where he or she "is not in a position to become aware of the loss, theft or misappropriation of the payment instrument".[143] Another operating principle of the Directive declares that once a consumer has notified a payment service provider that their payment instrument may have been compromised, the consumer "should not be required to cover any further losses stemming from unauthorized use of that instrument".[144]

Therefore, under the Directive, a card user whose card is lost or stolen or misappropriated will be liable for all the losses relating to any unauthorized payment transaction on an account linked to that particular card, where one of the following elements exists:

(1) where the card user acted with a fraudulent intent; or,
(2) where the card user failed to use the card in accordance with terms governing its issue and use, such as taking all reasonable steps to secure the card's personalized security details; or,

---

[131] *See* The Electronic Funds Transfer Act, United States Code: Title 15: section 1693q.
[132] *See* EU Directive on Payment Services 2015, art 64 (1).
[133] *See* EU Directive on Payment Services 2015, art 64 (2).
[134] *See* EU Directive on Payment Services 2015, art 71.
[135] *See* EU Directive on Payment Services 2015, art 73(1).
[136] *See* EU Directive on Payment Services 2015, art 74(1).
[137] *See* EU Directive on Payment Services 2015, art 74(1) (a).
[138] *See* EU Directive on Payment Services 2015, art 74(1) (b).
[139] *See* EU Directive on Payment Services 2015, art Article 74(1).
[140] *See* EU Directive on Payment Services 2015, art 64 (1) (a).
[141] *See* EU Directive on Payment Services 2015, art 64(2).
[142] *See* EU Directive on Payment Services 2015, art 64 (1) (b).
[143] *See* EU Directive on Payment Services 2015, para 71.
[144] *Ibid.*

(3) where the card user failed to timely notify the relevant payment service provider upon becoming aware of the loss, theft, misappropriation or unauthorized use of the card.

There are currently no provisions in the Cybercrime Act or the CBN's regulations that address for example the degree of a customer or bank's liability where a customer has reported that his or her electronic bank card or other confidential electronic banking information has been compromised as a result of negligence or other factors such duress or theft. Given this state of affairs, it will be helpful for Nigeria to consider adopting the above examples of the United States and the EU. Adopting the above examples will enhance certainty in the liability regime that applies to unauthorized payment transactions as a result of cybercrime which arise from the compromise of electronic bank cards or payment details due to negligence or other factors such duress or theft.

4 Challenges Impeding the Protection of Consumers from Cybercrime in the Banking and Financial Sector

Aside from the shortcomings that were identified in the legal analysis above, there are also several challenges that impede the protection of consumers from cybercrime in the Nigerian banking and financial sector. In this regard, a major challenge is the issue of poor public awareness regarding cybercrimes that target electronic banking and payment platforms. This lack of awareness can be traced to low levels of cybersecurity awareness due to poor consumer education as well as ineffective and poorly disseminated consumer enlightenment programs.[145] The problem of lack of awareness is further compounded by low levels of technology literacy. Many consumers lack basic knowledge on how to conduct electronic financial transactions[146] and have to seek the assistance of third parties which then results in the disclosure of confidential banking details such as the PINs of their bank cards. This lack of technology literacy also leads to situations whereby consumers may respond to unsolicited communications purportedly coming from banks or financial institutions but actually made by criminals, requiring them to disclose their personal banking details.

Addressing the issue of poor public awareness on cybersecurity threats that target electronic banking and payment platforms will require more effective and widely disseminated consumer enlightenment programs. In particular, it will be helpful if consumer enlightenment programs are used to constantly keep consumers aware of emerging trends of cybercrime that target electronic banking and payment platforms. Such programs may be disseminated through the use of mass media and telecommunication platforms, including SMS messages, emails and social media networks. In this regard, the CBN may establish obligations on banks and financial institutions to provide regular consumer education programs to their customers. A commendable initiative in this regard is the CBN's Circular on the Establishment of Industry Fraud Desks (2015) which requires banks to sensitize customers on electronic fraud and also provide support to customers on related issues, such as placing restrictions on accounts following complaints of fraud.[147]

The CBN's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers which was issued on 25 June, 2018, clearly recognizes the need for banks and payment service providers to promote cybersecurity awareness amongst consumers and employees.[148] Accordingly, the Framework requires banks and payment service providers to develop cybersecurity awareness trainings, and "communicate cybersecurity awareness to their customers in the language they understand; possibly in local dialect at least monthly or when there is an identified cyber-threat or attack vector".[149] The Framework also requires banks and payment service providers to devise mechanisms to communicate such cybersecurity awareness via SMS, emails, radio, newspapers and other mass media platforms.[150] The effective implementation and enforcement of the above obligations under the Framework will go a long way towards promoting consumer awareness of cybersecurity threats on electronic banking and payment platforms and thereby reduce the volume of consumer losses arising from cybercrime in the Nigerian banking and financial industry.

---

[145] *See* Onajite Regha, 'Aggressive Consumers Awareness Initiatives: A Proactive & Consistent Mechanism to Preventing E-fraud' in *Nigerian E-Fraud Forum 2015 Annual Report: Improving and Securing the Cyber Environment* (Central Bank of Nigeria 2015) 10–13.

[146] *See* Ifeanyi Chris Onodugo, 'Overview of electronic banking in Nigeria', *International Journal of Multidisciplinary Research and Development* (2015)2 (7)340; U Kama and M Adigun, 'Financial Inclusion in Nigeria: Issues and Challenges', *Central Bank of Nigeria Occasional Paper* (August, 2013) (45)31–33.

[147] *See* Central Bank of Nigeria, *Circular on the Establishment of Industry Fraud Desks*, BPS/DIR/GEN/CIR/02/004 (11 June, 2015).

[148] *See* Central Bank of Nigeria, *Draft Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers* (25 June, 2018) 18–19 at Appendix III, para 3.

[149] *See* Central Bank of Nigeria, *Draft Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers* (25 June, 2018)19 at Appendix III, para 3 (e).

[150] *Ibid*, at 19, Appendix III, para 3 (f).

It should be noted that the Nigerian Consumer Protection Council Act,[151] which creates a legal and regulatory framework for the protection of consumers in Nigeria, also applies to services such as electronic banking and payment services. Under the Act, the CPC can compel a service provider to provide relief and compensation to consumers who have been injured by the effects of adverse technologies.[152] For example, a bank customer can obtain remedies through the CPC in the case of losses arising from an unauthorized payment transaction on his or her account due to the bank's failure to adequately protect its electronic banking and payment platforms. However, the existence of the Consumer Protection Act has not had significant impact on the protection of consumers that use electronic banking and payment platforms. This state of affairs appears to arise from the CPC's lack of requisite institutional regulatory capacities such as qualified manpower and technical capacities to address consumer issues relating to electronic banking and payments. Although, the CPC has expressed interest in protecting electronic card users by indicating its readiness to commence legal proceedings against banks that fail to compensate victims of cybercrime such as ATM fraud,[153] however, the CPC did not establish any regulatory directives in that regard and no banks have been prosecuted. There is also the challenge of limited consumer access to CPC's consumer redress mechanism, as many consumers do not stay in areas where they can easily access the CPC's consumer redress mechanisms, and the option of traveling long distances to lay complaints that involve small claims usually discourage consumers from seeking redress.[154] Also, when the costs of redress is weighed against a small consumer claim and the time that will be spent on the dispute resolution process, consumers are usually more inclined to abandon the option of seeking redress.

There is need for the government to enhance the CPC's technical and institutional regulatory capacities to address consumer issues related to the use of electronic banking and payment platforms. This will go a long way towards enhancing consumer trust in the effectiveness of the CPC's consumer redress system. Also, given that consumer complaints, which arise from issues related to the use of electronic banking and payment platforms (including consumer complaints that relate to cybercrime), may involve small claims and thereby lessen the incentive for consumers to seek redress, it is therefore imperative for the CPC to promote the enforcement of consumer rights and claims. The CPC can achieve this by exercising its regulatory powers to institute actions on behalf of consumers, or by encouraging civil society organizations to institute class action suits that seek to address common consumer complaints, including those that arise from cybercrime on electronic banking and payment platforms.

5 Concluding Remarks

Cybercrimes that target electronic banking and payment services generally reduce consumer trust in electronic transactions and also impedes the adoption and penetration of electronic banking and payment services as well as e-commerce. This also has the effect of limiting the social and economic development prospects of information communication technologies in developing countries such as Nigeria. Although, Nigeria has taken a commendable step by establishing the Cybercrime Act to protect consumers that use electronic banking and payment platforms in the banking industry, there is still a need for further responses as highlighted in this paper. In particular, it will be helpful for Nigeria to consider drawing lessons from the highlighted examples of legal regimes in the United States and the EU in order to strengthen the protection of consumers that use electronic banking and payment services. More importantly, the Nigerian Cybercrime Advisory Council which is established under section 42(1) of the Nigerian Cybercrimes Act has powers to formulate guidelines for the implementation of the Act.[155] In this regard, the Council can make guidelines that will impose a greater or strict liability regime on banks and financial institutions under section 19(3) of the Cybercrimes Act, so that they can have a higher degree of liability for the breach of consumer data. The Council can also establish guidelines that will address the degree of a customer or bank's liability where a customer has reported that an electronic bank card or other confidential electronic banking or payment information, have been compromised as a result of negligence or other factors such duress or theft. Another option is for the Attorney General of the Federation to exercise the powers under

[151] *See* The Nigerian Consumer Protection Council Act, Cap. C25 LFN.

[152] *See* Nigerian Consumer Protection Council Act, s 2.

[153] *See* Victor Oluwasegun and Dele Anofi, 'Reps, CPC Probe Banks over Malfunctioning ATMs', *The Nation* (4 June, 2013) <http://www.thenationonlineng.net/reps-cpc-probe-banks-over-malfunctioning-atms/>; PM News, 'ATM Fraud: CPC, NBA Set to Tackle Banks', PM News (24 August, 2010), available at <https://www.pmnewsnigeria.com/2010/08/24/atm-fraud-cpc-nba-set-to-tackle-banks/> accessed 5 November, 2018.

[154] *See* Orji, (n 24)353.

[155] *See* Cybercrimes (Prohibition and Prevention, etc) Act, 2015, s 43(1)(b).

section 57 of the Act with a view to making guidelines that will address the identified shortcomings of the consumer protection regime under the Act. In addition, the CBN can exercise its powers to regulate the banking and financial sector[156] in order to make regulations that will strengthen the consumer protection regime under the Cybercrimes Act. Finally, it is also imperative that regulatory developments are timely initiated to address highlighted gaps in the consumer protection regime under the Act so as to further enhance certainty and consumer trust in the use of electronic banking and payment services in Nigeria.

Competing Interests

The author has no competing interests to declare.

[156] *See* Banks and Other Financial Institutions Act, 1991 (As Amended) s 1, 2, 3, 5, 31–39. *See* s 1(3) and 2(d) Central Bank of Nigeria Act, 2007, *Official Gazette of the Federal Republic of Nigeria* (1 June, 2007) 94, Government Notice No. 34, A63-19.

How to cite this article: Uchenna Jerome Orji, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria' (2019) 24(1) *Tilburg Law Review* pp. 105–124. DOI: https://doi.org/10.5334/tilr.137

Published: 21 February 2019

]u[*Tilburg Law Review* is a peer-reviewed open access journal published by Ubiquity Press.

OPEN ACCESS