# Cybercrime and Digital Transactions Law in Nigeria: A Review

**Ngozi Chisom Uzoka and Nneka Obiamaka Umejiaku**
Department of Private & Property Law, Faculty of Law, Nnamdi Azikiwe University Awka, Nigeria.

nc.uzoka@unizik.edu.ng
no.umejiaku@unizik.edu.ng

**Abstract:** The internet is a tool that drives globalization and enhances global inclusion and integration. It has become imperative to make use of information and communication technology in this era of increased broadband access to the internet. The use of information and communication technology has increased the commission of cybercrime such as data breaches, identity theft and cyber fraud. This paper aims to identify the relevance, authenticity and nexus between digital transactions and cybercrimes in Nigeria. This paper seeks to give a summary of cybercrime and digital transaction laws in Nigeria, as well as the challenges inherent in applying them. The methodology adopted is the doctrinal method of legal research approach in literature review, analysis of cases and access to internet sources. This paper made use of primary sources of data such as such as enabling laws, acts and secondary sources of data, conventions, journal articles and the study is also analytical and comparative in nature. The paper finds that the legal and institutional framework for digital transaction laws in Nigeria is somewhat limited. Some digital forensic tools have not been recognized by our laws in Nigeria. The paper concludes that the extant legal framework for digital transaction laws in Nigeria has lapses that impair the evidence emanating from digital tools/records. This paper recommends amongst others; training of prosecution officers, legal practitioners and judicial officers in the collection and use of forensic/digital evidence in court of law, review of some of our extant laws and creation of institutional framework for digital transaction laws in Nigeria.

**Keywords:** Digital law, Cybercrime, Justice, Electronic law, Electronic evidence, E-commerce

## 1. Introduction

Two decades ago, many people did not have mobile phone or computer as a result of the cost. Connecting to the internet was only accessible through dial-up modems. In Nigeria before now, people pay hourly or by minutes to access the internet in cyber cafes. The use of electronic mails was not common as well as the electronic banking systems. Presently, many individuals now own laptops, mobile phones that can connect to the internet and email accounts effortlessly wherever they are. Presently, there are many social media platforms where people can connect easily with others without physically meeting. Individuals now frequently purchase goods online and are increasingly using electronic readers for books and newspapers rather than traditional print media.

Over two decades there has been an increased usage of technological inventions which has provided platform for its misuse and crimes. This has increased the use of technology by individuals to create new forms of crimes. With the emergence of information and communication technology and the growing usage of internet on daily basis, there are now many avenues through which cybercrimes can be carried out. “Individuals who engage in socially unacceptable or outright criminal acts steadily make use of technology to connect with one another in ways that is not before now possible” Holt,T. J. , Bossler A. M., Seigfried – Spellar, K.C (2015). Because of the possibility of carrying out transactions online without any physical meeting, persons have taken undue advantage of that to perpetuate and engage in all sorts of cybercrimes. As a result of the differences in jurisdictions, there is no generally acceptable definition of cybercrime that is all encompassing. Cybercrime is challenging to conceptualize with exactitude. However, one factor remains constant in various definitions given by scholars. Cybercrime is a crime that is committed over the wireless internet. On the other hand, cybercrime can be termed as any crime or criminal activity executed by making use of digital technology, or put differently they are computer-related crimes and crimes related to the internet. Digital technology and electronic networks provides an enviable platform to promote commercial transactions across the globe. A major sector of the economy that has robustly been affected positively or negatively by the intrusion of digital technology is the banking sector. Digital banking has facilitated a great deal digital transactions hence sellers and buyers of goods and services leverage on digital technology to initiate and conclude their transactions without any physical meeting. Thus, it is without doubt that in Nigeria and the world at large, financial technology has provided a formidable platform for digital banking operators to provide a wide range of financial services. This has in turn opened the door for an influx of various types of cybercrimes.

### 2.1 The Relevance of Digital Transactions to Cybercrime

Owing to the internet’s globalization and trans-border nature of digital transactions, cybercrime can occur anywhere. It suffices to state that there would be no cybercrime, if there was no internet. With the ease and

access to the internet by all and sundry in Nigeria coupled with the availability of different network providers of internet accessibility, digital transactions are on the increase. Years back the main medium of payment in Nigeria was basically cash. This has led to a lot of vulnerabilities and loss occasioned by robbery, theft etc. Subsequently, banks and other businesses introduced the use of Automated Teller Machines (ATM), Point of Sales (POS) and bank apps. As more people make use of the internet to transact business, there is a higher risk of being victims of cyber-attacks like online fraud, identity theft, and spyware or virus attacks. (Rathna *e tal*, 2023). The faster with the adoption of new payment systems, the more rapid and sophisticated the cyber risks are. A secured payment is paramount for any business that relies on electronic payments and transactions. If the digital payment system is weak, then it will be prone to constant attacks by cyber criminals. The negative consequences of cybercrime are vast and are a growing cause of global concern. The COVID - 19 pandemic also helped to facilitate companies to digitize their products and services, migrate to electronic commerce platforms and leverage on online business continuity strategy.

Cybercrime is not only evident in Nigeria, but also a global menace. Studies have estimated a yearly 15 per cent increase in global cybercrime losses over the next five years reaching 10.5 trillion US Dollars annually by 2025(Business day Newspaper Nigeria 2022). In Nigeria, over 2,800 persons were convicted of cybercrime in 2022(Queen Troanusi 2022). The increase in cybercrimes in Nigeria is highly attributed to the development and improvement of the internet. The development of the Electronic Data Interchange which replaced the traditional mailing of documents with a digital transfer of data from one computer to another enhances the transfer of orders and other transactions. Thus EDI allows the transfer of data seamlessly without any human intervention. With digital transaction, people can transact business from any part of the world without really verifying the authenticity of the other party. This is a major threat of transacting business electronically/digitally. On the other hand, electronic/digital transaction platforms, provides the buyer and the seller a wide range of database of services and products from which to choose from within a short time. It also eliminates the need for an agent or middleman; this will in turn reduce to some extent the risk of counterfeit and adulterated products as there is a direct channel between the producer and the consumer.

## 2. Digital Transactions in Nigeria

Generally, a lot of services or goods can be rendered or purchased digitally. Thus, an electronic transaction is the buying and selling of goods and services online. Additionally, conducting major and essential elements of a contract or any business whether commercial or non-commercial in nature via communications transmitted through digital devices will qualify the transaction as an electronic one. The term digital transaction can be used inter-changeably with the term 'electronic commerce'. Electronic commerce has no universal definition. However, it has been defined as commercial transactions conducted electronically on the internet. (OECD 1997 Report) In Nigeria, the total transaction value in the digital payments market is projected to reach US $21.32bn in 2024. Presently, Nigeria's digital transactions revolution is driving economic growth and financial inclusion at unprecedented levels (NASDAQ: ACIIN, 2022). While cash is still in use in Nigeria, there is a paradigm shift towards the adoption of digital payment systems. It is proven through research that governments that advance their national payments system create an enabling environment for everyone in the payments (Santhosh Rao).

## 3. Digital Transactions Regulation in Nigeria

### 3.1 Legal Framework for Cybercrimes and Digital Transactions in Nigeria

Digital or electronic transactions have raised a lot of germane novel issues with respect to control and regulation. The issue of validity, security and enforceability of digital transactions is vital.

#### *3.1.1 Evidence (Amendment Act) 2023*

Evidence Act is one of the principal legislation used in Nigerian courts. It has been subject to some amendments as a result of evolving legal system and the need to keep up with international best practices. The Evidence (Amendment) Act of 2023 brought significant changes in Nigeria's legal jurisprudence. However, it remained largely unchanged with respect to the inadmissibility of electronically generated evidence. Hence, there was need to address the lacuna in the Act to reflect technological realities in the world today. Under the erstwhile Evidence Act of 2011, the admissibility of computer generated evidence was introduced under Section 84. The 2011 Act also defined a document as including any devise by means of which information is recorded, stored or retrievable including computer output (Section 258). However, more was needed to improve the admissibility

of evidence, particularly electronically generated evidence as contained in the Evidence Act of 2011. Hence, the Evidence (Amendment) Act of 2023 introduced novel digital and electronic execution of documents and admissibility of storage mediums as evidence.

The Evidence (Amendment) Act of 2023 indeed contains visible provisions geared towards digitization of transactions and processes which will find expression in various fields and sectors, ranging from business contracts, financial transactions, government documents and healthcare records. The Federal government in Nigeria, in its bid to combat the overwhelming increasing rage of cybercrimes in Nigeria, as well as to protect the digital space has enacted a few legislations in this regard. Under the erstwhile Evidence Act of 2011, the admissibility of computer generated evidence was introduced under Section 84. The 2011 Act also defined a document as including any devise by means of which information is recorded, stored or retrievable including computer output (Section 258). However, more was needed to improve the admissibility of evidence, particularly electronically generated evidence as contained in the Evidence Act of 2011. Hence, the Evidence (Amendment) Act of 2023 introduced novel digital and electronic execution of documents and admissibility of storage mediums as evidence.

Under the new Nigerian Evidence (Amendment Act) of 2023, electronic record is defined to include "data, record or data generated image or sound stored, received, or sent in an electronic form or micro film" (Section 84). The word "electronic record" has been specifically inserted after the word "document" throughout the entire section 84 that deals with computer-generated evidence in the Act. This implies that documents or electronic record satisfies the laid down conditions of the Act. Specifically, Section 10 of the Evidence (Amendment Act) 2023, provides that electronic records printed on paper, stored and recorded or copies in optical or magnetic media or cloud computing database produced by a computer are now admissible in any judicial proceeding before Nigeria courts without further proof or production of the original, if the conditions enumerated in the Act are met. This provision was not contained under the previous 2011 Evidence Act. The 2023 Evidence Act introduced the use of digital signature in legal documents. Under section 10 of the new Act, It went further to define digital signature as one that is generated electronically and attached to a document that is electronically transmitted in order to verify the contents or authenticity of the document and the identity of the sender. In the same vein, the Act now recognizes the use of digital signatures in court documents or legal processes.

The advantages of digital and electronic signatures cannot be overemphasized. Digital and electronic signatures provide a higher level of security. They use encryption technology in order to ascertain the integrity and authenticity of the signed document. This will forestall forgery, tampering and alterations. Electronic signature also facilitates speedy transactions as there will be no need for physical paperwork printing or mailing. Court processes, land transaction documentations, contractual documents can also be signed by parties electronically and transmitted same way. This will facilitate faster court processes; times spent on perfecting agreements and ultimately increase efficiency. With digital and electronic signature parties to a transaction can afford to sign or access the documents from anywhere at any time. There would be no need for physical meeting by parties. Hence, this will facilitate trans-border and international transactions. Digital and electronic signature will create an enabling environment for audit trail. It easily provides a comprehensive record of when, who and how a document was signed will be on record. This will promote accountability and will be handy in the resolution of any discrepancies that may arise in the future (Ayojimi, 2024).

### *3.1.2 Cybercrimes (Prohibition, Prevention e.t.c.) Act 2015*

This was enacted by the National Assembly to ensure an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Cybercrime Act was signed into law in 2015. The Act contains 59 sections, is divided into 8 parts and it has two (2) schedules. The Act applies throughout the Federal Republic of Nigeria. The implication is that any other law made in respect of Cybercrime by a State House of Assembly is void or inactive, as the case may be. It is worthy to note that cybercrimes may take different forms, but the impact on electronic transactions is enormous, be it electronic commerce, electronic governance, electronic education or any other forms of electronic transactions, hence, several provisions of the Cybercrimes Act relate to an electronic transaction.

Under the Act, the term "cybercrime" was not defined at all. This leaves the meaning and scope of what constitutes cybercrime in Nigeria to speculation. Also under Section 48 of the Act, a law enforcement officer may apply *ex-parte* to a judge in chambers for the issuance of a warrant for the purpose of obtaining electronic evidence related to crime investigation. The judge is to issue a warrant authorizing law enforcement officer to

enter and search any premises or place if within those premises, place or conveyance an offence under Act is being committed, or there is evidence of the commission of an offence under the Act; or there is an urgent need to prevent the commission of an offence under Act.

Under Section 6(1) of the Act, it is an offence for any person without authorization to intentionally access in whole or in part, a computer system or network for fraudulent purposes and obtain data that are vital to national security. It is an offence under the Act to intentionally obtain computer data, secure access to any program, commercial or industrial secrets or classified information (Section 6(2)). It is an offence under the Act to unlawfully intercept data or to either directly or indirectly modify or cause the modification of any data held in any computer system or network by way of alteration, erasure, removal, suppression or prevention of the normal operation of the computer system or network (Section 16(1). Under the Cybercrime Act, it is an offence to use any device for the purpose of avoiding detection or otherwise prevent identification or attribution with any of these acts or omission (Section 6(3).

The Act under Section 7 made it mandatory for all operators of cybercafés to register with Computer Professional Registration Council in addition to being registered as a business name with the Corporate Affairs Commission. The Act also mandated all cybercafé operators to maintain a register of users through sign-in personnel whenever needed. Section7 subsection 2 also provides that any person who perpetrates electronic or online fraud using a cybercafé commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of N342, 000,000.00 or both. The question is whether this can be implemented as most cybercafés in Nigeria as not even registered as a business name with Corporate Affairs Commission not to talk of registering with Computer Professional Registration Council. It is submitted that this will amount to a clog in the wheel particularly in the area of enforcement. The inclusion of CPRC in the enforcement realm will amount to decentralization of the enforcement framework. It is submitted that it will be most appropriate to have a single enforcement institution to fight against the menace of cybercrime in Nigeria. (Nwafor, 2022)

Another striking provision of the Cybercrimes Act is that it is an offence for any person to destroy or abort any electronic mails or processes through which money or any valuable information is being conveyed (Section 9).The Act is silent on what the term “valuable information” means. This makes room for guessing and speculation. There is a duty imposed on financial institutions to safely guard their customer’s sensitive information.

Under Section 17(1) 9 (Cybercrimes Act 2015), electronic signature with regards to purchases of goods and services, and any other transactions shall be binding. No transaction would be denied enforceability simply because the transaction was electronically signed. Whenever the genuineness or otherwise of electronic signatures is in question, the burden of proof that the signature does not belong to the purported originator of such electronic signature shall be on the contender (Section 17(1) a).

The Act also provided that any person who with the intent to defraud or misrepresent, forges through electronic devices another person’s signature or the mandate of a company commits an offence. The said offence is punishable with imprisonment for a term of not more than seven years or a fine of not more than N10 million naira or both fine and imprisonment (Section 17(1)c).

However, under the Act there are exemptions to transactions that can be electronically signed for example: death and birth certificate, wills, family law matters and

Under Section 37 of the Act, financial institutions are mandated to verify the identity of their customers carrying out electronic financial transactions and execute the documentation of customers preceding the execution of customers’ electronic transfer, payment, debit and issuance orders. (Section 37(1) a &b. This section is to ensure that financial institutions uphold an effective mechanism against financial malpractices where banking transactions are involved. It ushers in a new dawn in electronic commercial transactions in the financial world due to the duty of care imposed on financial institutions. Additionally, Section 38 of the Act mandated service providers to keep all traffic and subscriber information as may be prescribed by the relevant authorities responsible for regulating communication services in Nigeria for 2 years. Service providers are required to retain content and non-content information and make such available to an authorized law enforcement officer. The Act mandates that any data retained shall only be used for legitimate purposes as may be provided for under the Act, any other legislation, regulation or by order of a court of competent jurisdiction. Appropriate measures to safeguard the confidentiality of the data retained must be taken and the individual’s right to privacy under the Nigerian Constitution respected.

*3.1.3 Nigeria Data Protection Act 2023*

The Federal Government of Nigeria in an effort to regulate personal data in Nigeria enacted the Nigeria Data Protection Act 2023 also known as the (NDPA), this comes after the Nigeria Data Protection Regulation issued by the National Information Technology Development Agency(NITDA) in 2019. This Act replaced the erstwhile Nigerian Data Protection Regulations (NDPR) 2019 and the Nigerian Data Protection Regulations Implementation Framework 2019 which was issued under the National Information Technology Development Agency (NITDA). This present Act of 2023 established the Nigeria Data Protection Commission.

The NDPA basically applies to the processing of personal data by a data processor whether automated or not, that belongs to data subjects in Nigeria. It is pertinent to note that it is immaterial whether the data controller or data processor is not operating in Nigeria. However, as long as the data subjects are domiciled in Nigeria, surely the NDPA must apply. Where Nigerian citizens are residing outside Nigeria, the NDPA will not protect them. It is worthy to note that there are circumstances under the Act where the NDPA will not apply to a data controller or data processor.

The exceptions include:

a. the prevention, investigation, detection, prosecution, or adjudication of a criminal offense or to execute a criminal penalty in accordance with any applicable law;
b. to prevent or control a national public health emergency;
c. as is necessary for national security;
d. in respect of publication in the public interest, for journalism, educational, artistic and literary purposes to the extent that such obligations and rights incompatible with such purposes; or
e. necessary to establish exercise, or defend legal claims, whether in court proceedings, or in an administrative or out-of-court procedure.

It is pertinent to state that all digital businesses and platforms are under obligation to abide by the legal and regulatory requirements under the Act or face the penalty contained therein.

## 4. Challenges Associated with Enforcement of Digital Transaction Laws in Nigeria

Firstly it is paramount to note that in Nigeria we have a limited number of legislations with regards to regulation of electronic transactions as well as proliferation of cybercrimes. In addition, the existing legislations did not make any provisions or adequate consumer protections with respect to regulating tech giants digital payments and smartphone wallet services in Nigeria.

Secondly, our enforcement mechanism is very poor in Nigeria. Government bodies that are charged with compliance with the statutory provisions of the law are inefficient. Most of the agencies for enforcement are bedeviled by corruption and corrupt practices.

Defaulters to the provisions of our extant legislation must be punished adequately so as to deter would be offenders from venturing into same. Non-compliance should be taken seriously.

Members of the public should be sensitized about their rights under the various legislations. There should be a massive awareness program by government, government agencies, non-profit organizations and a host of civil society groups on the provisions of the novel laws that are being made in Nigeria. Creation of awareness on how cybercriminals operate will in no small measure reduce the exposure of unsuspecting members of the public to falling victim to cybercrimes

Additionally, data controllers as well as data processors are to ensure strict compliance with the letters and intendment of the laws, this will exonerate them from liabilities.

## 5. Conclusion

It is glaring that the digital era has posed a lot of legal challenges in Nigeria. It has also exposed the lacuna in our present laws. As the years unfold, the scope of cybercrime is growing rapidly, as countries attempt to beef up and proactively secure their digital payment system laws, the threat of cyber fraud continues, hence the urgent need for novel changes in our laws. An increase in cybercrime is a global menace as well as double jeopardy to Nigeria's businesses and its citizens. There is an urgent need to enhance growth genuineness and sustainability of digital transactions through effective and adequate legal frameworks.

Even though the Nigerian government recently has taken steps to bridge the gap in our legal framework with respect to digital transaction processes; as well as protect its citizens against fraud, much still needs to be done. At the international level, electronic or digital transaction has gained so much prominence that it has specific laws regulating it. For example, the United States has the Electronic Signatures in Global and National Commercial Act 2000 and the Uniform Electronic Transactions Act at the State level. Also in United Kingdom, they have the United Kingdom's Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002. In South Africa, there is Electronic Communications and Transactions Act 2002.

## 6. Recommendations

Cyber security and cyber warfare is a continuum. The digital space is no longer a lawless frontier; rather nations of the world are now alert to making laws to ensure that the cyber space is safe. It is pertinent to state that digital transactions is the foundation of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies.

In Nigeria, there is an urgent need to have a legal framework dedicated solely to regulation of electronic or digital transactions as is obtainable in some other jurisdictions. There is no law in Nigeria that is dedicated to this urgent precarious situation; this has to a great extent hindered the ease of doing business in Nigeria. There is also the need to consider the recognition of electronic identification, authentication and trust services in the African region that would recognize the legal validity of digital signatures and stamps and as well as their admissibility as evidence across member states. This will enhance trade relations across the continent.

The government of Nigeria needs to create and or establish a digital or electronic systems regulator. They should be charged with statutory duties to promote innovation and ensure that digital/electronic transactions are operated and conducted in a way that promotes the interests of businesses and consumers. Individuals should be able to express and engage freely on the internet; having the confidence that their personal data will also be protected.

The Nigerian government should organize educational campaigns to educate, sensitize and inform the public about the benefits and dangers of electronic or digital payment systems. People should be taught on how to seal deals electronically, how to do use digital payment methods and how to detect cyber-fraudsters.

On a global scale, there is an urgent need for countries on international and regional levels to drive greater interoperability and inclusivity with a view to coherent and efficient regulatory reforms for digital payment systems.

The Nigerian Judiciary should embrace the use of electronic evidence as a means to administration of criminal justice. The judges, legal practitioners, public prosecutors should be trained, be proactive and embrace the use of digital forensic tools. Thus digital forensic tools are applications and devices that are geared towards facilitating the investigation and analysis of digital evidence. This will improve the efficiency and effectiveness of our justice delivery system in Nigeria.

Conclusively, the world must together take note of the inherent challenges of criminals into the cyberspace and work towards harmonized national and international policies so as to synergize the war against cybercrimes and a safe cyber space for digital transactions.

## References

Ayojimi, M. (2024) 'The Evidence Act of 2023: A Remarkable Advancement in Nigeria's Jurisprudence," Available at www.lawpavillion.com Jan 10.

Digital Forensics 1st ed Edited by Andre Arnes 2018 John Wiley & Sons Ltd.

Digital Payments – Nigeria, Available at www.statistic.com accessed on 23/01/2024.

Hoar, S.B. , (2001) Identity Theft: The Crime of the New Millennium , Or. Law Rev. 80, 1423.

Holt, T. J. , Bossler A. M., Seigfried – Spellar, K.C.(2015) *Cybercrime and Digital Forensics: An Introduction* Routledge, United Kingdom.

International Strategy for Cyberspace: prosperity, security, and openness in a Networked World, (2011). USA.

Lubis, M. and Handayani, D.O.D., 2022. The Relationship of personal data protection towards internet addiction: Cyber crimes. Pornography and reduced physical activity. Procedia Computer Science, 197, pp 151-161.

Nwafor, E.I.,(2099) *Cybercrime and the Law: Issues and Development in Nigeria,* Kraft Books Limited, Nigeria.

Nigeria Recorded a 174% increase in Cybercrimes in six months; November 18, 2022, Business Day www.businessday.ng.

Onuora A C, Uche D C. et al, The Challenges of Cybercrime in Nigeria: An Overview, AIPFU Journal of School of Science Vol. 1 No. 2 2017.

Organization for Economic Corporation and Development (OECD) report on Electronic Commerce: opportunities and challenges for Government OECD, 1997) at P.20
Prime-Time for Real Time 2022 3rd edition published by AU Worldwide, (NASDAQ: ACIIN)
Queen Troanusi, over 2,800 persons convicted of cybercrime in 2022 – EFCC. www.premiumtimesng.com
Rathna, G., Mohan, S., Jayalakshmi, J. S., (2023) *Cybercrime and Digital Payments In India: A Comprehensive Analysis*, India.
Santhosh Rao, Head of Middle East, Africa and South Asia, ACI Worldwide.