# CONSUMER TRUST AND THE ROLE OF DIGITAL FORENSIC IN SECURING NIGERIA'S E-COMMERCE SYSTEM

**By**

**Dr Baribefe-Koate, Maureen***
**Chigoziem, Ekeno Solomon****
**Juongwa, Kingsley Nnaemeka*****

***Abstract***

*The rapid expansion of e-commerce in Nigeria had transformed retail and service delivery, yet it faced persistent challenges related to cybercrime, data breaches, and online fraud, which undermined consumer trust. This paper examined the role of digital forensics as a strategic tool for securing e-commerce platforms, enhancing consumer confidence, and ensuring compliance with Nigeria's legal and regulatory frameworks, including the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024) and the Data Protection Act 2023. It explored key digital forensic techniques, such as network, database, mobile, cloud, and AI-assisted forensics, and highlighted their applications in fraud detection, breach investigation, cybersecurity policy enhancement, and legal evidence collection. The challenges included limited expertise, high costs, and evolving cyber threats, along with actionable recommendations for capacity building, tool adoption, consumer education, and stakeholder collaboration. It concluded that integrating digital forensic practices into Nigeria's e-commerce ecosystem is essential for mitigating cyber risks, strengthening regulatory compliance, and fostering sustainable consumer trust, thereby supporting the growth of secure and resilient online marketplaces.*

**Keywords:** *Digital Forensics, E-Commerce Security, Consumer Trust, Nigeria, Cybercrime, Data Protection.*

## 1. Introduction

In the 21st century, e-commerce emerged as a transformative tool in global trade which has reshaped traditional business models, commercial practice, retail system, payment system and consumer behaviors with e-commerce platforms like Jumia, Konga, Paystack and others dominate in Nigeria. Besides, this growth has been greatly affected by the rise in cyber threats, posing significant challenges on security, integrity, and public trust which are essential tools for substantial e-commerce development.[1]

A report by the Guardian Newspaper stated that cyber-attacks against Nigerian businesses most especially e-commerce platforms increased by 81% between 2021 to 2023[2] costing Nigeria $9.3 billion[3] and calls the urgent need for legal reforms and judicial adaptation.[4] In Nigeria, cyber-attacks has evolved from relatively simple internet fraud like "Yahoo Yahoo" scheme also known as "419" into more complex crimes like data breaches, identity theft,

* Dip (Law), LLB, BL, LLM, Ph D, PNMS, Lecturer and Head of Department, Public Law, Faculty of Law, Clifford University (Ihie Campus) Owerrinta, Abia State. Tel:+23407032390517, Email: maureenb@cliffordduni.edu.ng, maureenbkoate@gmail.com
** LLB, BL, LLM (in view) Lecturer, Faculty of Law, Clifford University (Ihie Campus) Owerrinta, Abia State Phone: 08027896691, Email; ekedear008@gmail.com
** Dip (Criminology & Security Studies), LLB, BL, LL.M (in view) Lecturer Faculty of Law, Clifford University Owerrinta (Ihie Campus) Owerrinta, Abia State. E-mail : juongwa1@gmail.com. Phone +2348169573573

[1] Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (as amended) 2024, s32

[2] E Nzor, 'Cybercrime Threatening Nigeria's Growth' *The Guardian* (Abuja: 23rd September, 2025)

[3] T Opaluwa, 'Cybercrime in Nigeria: The Fights Rages On' *The Leadership* (Lagos: 27th February, 2016)

[4] J Folaju, 'Cyber-attacks to be More Intense in 2025-Expert Warns' *The Guardian* (Abuja: 17th January, 2025)

phishing, ransomware, unauthorized system intrusions, etc. have resulted in threatening consumer trust and e-commerce growth.[5] Cyber-attackers use various methods to access people's networks and organization's network without authorization and this attacks might be active that is the brute-force attack which requires user's password or passive that is web-based attack whereby users are made to visit a malicious webpage in an attempt to infect the user's computer with malicious code with the motivation of gaining financial gain, stealing sensitive information, disable a network, establishing a command and control server, or using the system as a launching point for future attacks.[6] The success of cyber-attacks is dependent on poor security habits of the public in exposing their personal and sensitive data as strong passwords are not enough to prevent cybercrime due to vulnerability to breach of data.[7] According to statista, the global cost of cybercrime is projected to rise from $9.22 trillion in 2024 to $ 13.8 trillion by 2028.[8]

Formally, courts in Nigeria struggled with the admissibility of electronic evidence until the case of *Kubor v. Dickson*[9] where the court affirmed that electronically generated evidence is admissible provided it satisfies the conditions stipulated[10] and must conform to constitutional safeguards, particularly privacy rights.[11] Although, this reform are under-enforced due to limited forensic capacity and lack of trained judicial personnel, leaving victims of cyber-attacks

---

[5] I Suleiman, 'Digital Forensics as a Panacea to Cybercrime in Nigeria: Challenges and Prospects' *Benue State University Journal of Law* [2024] (12)(1) 88-101

[6] A Cruz, 'Cybercrimes and How it Affects You' *Cyber Security Tip*s [2013](7)(1) 14

[7] A O Ayub & L Akor, 'Trends, Patterns and Consequences of Cybercrime in Nigeria' *Gusau International Journal of Management and Social Science* [2022](5)(1) 243

[8] M Moore, 'Top Cybersecurity Threat to Watch in 2026' [2026] *University of San Diego* 1

[9] (2013) LPELR-20752 (SC)

[10] Evidence Act 2011 (as amended 2023), s84

[11] Constitution of the Federal Republic of Nigeria 1999 (as amended 2023), s37

without sufficient legal remedies.[12] Nwafor, went ahead to contend that the judiciary understanding of digital forensic science remains rudimentary, thereby affecting the quality of justice delivered in cybercrime cases.[13]

This action made digital forensics to be recognized as a key tool for securing e-commerce platforms, investigating cyber incidents, and preserving legal evidence[14] by providing insights into attack vectors, tracing fraudulent transactions, and enabling compliance with regulatory frameworks such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024) and the Data Protection Act 2023, digital forensics enhances both platform security and consumer trust.[15]

Furthermore, it is argued that consumer trust is strongly correlated with perceived security, privacy protection, and reliability of online services.[16] Integrating digital forensic mechanisms into e-commerce operations therefore not only supports the detection and mitigation of cyber threats but also reinforces consumer confidence, legal compliance, and overall market credibility.[17] Given the increasing frequency and sophistication of cyberattacks, the role of digital

---

[12] A O Olayemi, 'A Socio-Legal Study of Cybercrime and Its Implication in Nigeria' *Nigeria Law Journal* [2019] (14)(1) 89

[13] A O Nwafor, Digital Evidence and the Nigeria Legal System (1st edn; Lagos: Princeton Publishers, 2021) 5

[14] E E M Micah, I H Saidu, T Ibitomi & B S Sanusi, 'Digital Forensics in the Era of Cybercrime: Emerging Trends and Challenges for Forensic Accountants in Nigeria' *European Journal of Accounting, Auditing and Finance Research* [2023](11)(9) 85-100

[15] V Ishaya, 'Evaluating Law Enforcement Capabilities in Digital Forensics and Cyber Incident Management in Nigeria' *International Journal of Innovative Information Systems & Technology Research* [2025](13)(4) 322-339

[16] O Akinola, & O Ashaolu, 'A Trust, Privacy and Security Model for E-Commerce in Nigeria' *Nigerian Journal of Technology* [2023](42)(1) 152-159

[17] S Adeyemi, & T Olaniyi, 'Consumer Trust and Online Shopping Behaviour in Nigeria: The Role of Cybersecurity and Digital Forensics' *International Journal of E-Commerce Studies* [2020](11)(2) 88-102

forensics in Nigeria's e-commerce ecosystem has become indispensable, highlighting the need for policy interventions, capacity building, and technological investments. This paper seeks to explore how digital forensics can serve as a strategic tool to secure e-commerce platforms, mitigate fraud, and sustain consumer trust in the Nigerian context.

## 2. Conceptual Framework

An in-depth explanation on the concepts and terms adopted from the topic of this paper and how it identifies the subject matter.

### 2.1 Consumer Trust

Consumer trust is a central concept in understanding consumer behavior, particularly in electronic commerce where transactions occur without physical interaction between buyers and sellers. Trust is commonly defined as a consumer's willingness to rely on an online vendor or system based on the expectation that the seller will act competently, ethically, and securely.[18] In digital environments, trust serves as a mechanism for reducing uncertainty and perceived risk associated with online transactions.[19]

Accordingly, it can be said that consumer trust as a multidimensional construct comprising ability, integrity, and benevolence. Ability refers to the technical competence and operational capacity of an e-commerce platform to fulfill its obligations, while integrity relates to honesty, transparency, and consistency in adhering to stated policies and promises. Benevolence reflects the belief that the vendor will act in the consumer's interest and will not exploit the consumer's vulnerability.[20]

---

[18] R Mayer, J Davis & F Schoorman, 'An Integrative Model of Organizational Trust' *Academy of Management Review* [1995](20)(3) 709-734

[19] N Luhmann, *Trust and Power* (1st edn; Chichester: John Wiley & Sons, 1979) 1

[20] R Mayer, J Davis & F Schoorman, (n15)

In e-commerce systems, consumer trust is influenced by several technological and organizational antecedents. Perceived security and privacy protection significantly affect consumers' confidence in online platforms, as concerns over data breaches and fraud remain prevalent.[21] Secure payment systems, encryption technologies, and reliable website functionality enhance system quality and positively shape trust perceptions.[22] Therefore, vendor reputation, transparency, and previous satisfactory transaction experiences strengthen consumer trust and increase purchase intention.[23]

Institutional and legal safeguards also play a crucial role in reinforcing consumer trust. The existence of enforceable consumer protection frameworks and cybercrime legislation assures consumers that digital misconduct can be investigated and sanctioned, thereby increasing confidence in online transactions.[24] In Nigeria, compliance with data protection obligations under the Nigeria Data Protection Regulation further supports trust by ensuring lawful processing and safeguarding of personal data.[25] Oladejo stated a solution to the cyber threats on e-commerce platforms that restoring and maintaining consumer trust requires effective legal measures and technological solutions, including digital forensics, to detect, investigate and prevent cybercrimes.[26]

---

[21] D Gefen, E Karahanna & D Straub, 'Trust and TAM in Online Shopping: An Integrated Model' *MIS Quarterly* [2003](27)(1) 51-90

[22] P Pavlou, 'Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model' *International Journal of Electronic Commerce* [2003](7)(3) 101-134

[23] S McKnight, V Choudhury & C Kacmar, 'Developing and Validating Trust Measures for E-Commerce: An Integrative Typology' *Information Systems Research* [2002] 13(3) 334-359

[24] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended) 2024, s14-23; Nigerian Communications Commission, Consumer Code of Practice Regulations 2007, reg 32-35

[25] Nigeria Data Protection Regulation 2019, Article 2

[26] A Oladejo, 'Rebuilding Consumer Trust in Nigeria E-Commerce' *Journal of Cyber Law and Policy* [2022](3)(1) 28-41

## 2.2 Digital Forensics

Digital forensics refers to the application of scientific and investigative techniques to identify, preserve, analyze, and present digital evidence in a manner that is legally admissible. It plays a critical role in addressing cybercrime, electronic fraud, and data breaches, particularly within digital and e-commerce environments[27] as several branches of digital forensics are employed to extract and preserve evidence without compromising its integrity such as: computer forensics, network forensic, mobile device forensics, database forensics and cloud forensics.[28] Since commercial transactions increasingly rely on digital platforms, digital forensics has become essential for ensuring accountability, system integrity, and trust in online systems.[29]

Digital forensics is a structured process consisting of identification, preservation, examination, analysis, and presentation of digital evidence. Identification involves recognizing potential sources of digital evidence, while preservation ensures that such evidence remains intact and unaltered. Examination and analysis focus on extracting and interpreting relevant data, and presentation entails documenting findings for use in legal or administrative proceedings and this is fundamental to the credibility of forensic findings.[30]

Within e-commerce systems, digital forensics serves both reactive and preventive functions. Reactively, it supports the investigation of cyber incidents such as online fraud, identity theft, payment

---

[27] E Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd edn; USA: Academic Press, 2011) 4

[28] K Jones & R Valli, *Digital Forensic: Digital Evidence in Criminal Investigation* (1st edn; USA: Wiley, 2014) 12-35

[29] G Palmer, 'A Road Map for Digital Forensic Research' *Digital Investigation* [2001](1)(1) 27-30

[30] B Carrier & E Spafford, 'An Event-Based Digital Forensic Investigation Framework' *Digital Investigation* [2004](51)(2) 1-12

manipulation, and unauthorized access to consumer data.[31] Preventively, forensic readiness enhances an organization's capacity to detect suspicious activities early, preserve audit trails, and respond effectively to security breaches.[32] As noted by Brenner, without effective digital forensic investigation, cybercrime prosecution is nearly impossible due to the intangible and volatile nature of digital evidence.[33]

Digital forensics also has significant legal and institutional relevance. The admissibility of digital evidence depends on compliance with established forensic standards and legal procedures, including proper chain of custody and documentation.[34] In Nigeria, the relevance of digital forensics is reinforced by cybercrime and data protection regulations, which recognize electronic evidence and mandate lawful investigation of digital offenses.[35]

## 2.3 Cybercrime

Cybercrime refers to unlawful activities carried out through computers, digital networks, or internet-enabled devices, where technology serves as either the target or the instrument of the offense. With the rapid expansion of e-commerce and digital payment systems, cybercrime has become a major threat to the security, reliability, and credibility of online transactions.[36] In developing digital economies such as Nigeria, cybercrime poses

---

[31] N Beebe and J Clark, 'A Hierarchical, Objectives-Based Framework for the Digital Investigations Process' *Digital Investigation* [2005](2)(2) 147-167

[32] S Raghavan, 'Digital Forensic Readiness in Organizations' *Journal of Digital Forensics, Security and Law* [2013](9)(1) 45-62

[33] S Brenner, *Cybercrime and Digital Forensics* (5th edn; USA: Taylor & Francis, 2010) 56-58

[34] E Casey, (n23)

[35] Evidence Act 2011 (as amended 2023), s84

[36] D Wall, *Cybercrime: The Transformation of Crime in the Information Age* (1st edn; Cambridge: Polity Press, 2007) 7

significant challenges to consumer trust and the sustainability of electronic commerce platforms.

Cybercrime encompasses a wide range of activities including online fraud, identity theft, phishing, unauthorized system access, data breaches, and electronic payment manipulation. These offenses exploit vulnerabilities in information systems and human behavior, often resulting in financial loss, privacy violations, and reputational damage to both consumers and businesses.[37] The prevalence of such crimes increases consumers' perceived risk and reduces their willingness to engage in online transactions.[38]

According to Brenner, cybercrime is classified into two categories: cyber-dependent crimes (offences that can only be committed through computers, such as hacking) and cyber-enabled crimes (traditional crimes facilitated by digital technologies, such as fraud).[39] The types of cybercrime includes: cyberterrorism, malware, cyberstalking, spam or phishing, fraud-identity theft, logic bombing, email and SMS spoofing and password sniffing.[40]

From a conceptual standpoint, cybercrime functions as a negative external factor that undermines consumer trust in digital environments. Repeated exposure to cyber incidents erodes confidence in the safety of e-commerce platforms, even where technical security measures are present.[41] The perceived likelihood of fraud and lack of effective enforcement further intensify

---

[37] M Yar, *Cybercrime and Society* (2nd edn; London: Sage Publications, 2013) 12

[38] P Pavlou, (n19)

[39] S Brenner, *Cybercrime: Criminal Threats from Cyberspace* (1st edn; California: Praeger, 2007) 21-35

[40] M Olusola, O Samson, A Seminu & A Yinka, 'Cybercrime and Cyber Law in Nigeria' *The International Journal of Engineering and Science* [2023](2)(4) 19-25

[41] D Gefen, E Karahanna & D Straub, (n18)

consumer skepticism, particularly in jurisdictions with limited investigative and prosecutorial capacity.[42]

In Nigeria, Cybercrime (Prohibition, Prevention, etc.) Act 2015 (as amended 2024) is a primary legislation of Nigeria in combatting cyber offences, investigating powers, and penalties. With the act criminalizing unauthorized access to computer system or network[43] and cyber financial fraud[44] which are admissible in court.[45]

## 2.4 E-Commerce Ecosystem

E-Commerce ecosystem refers to the network of digital platforms, consumers, service providers, payment infrastructures, regulatory frameworks, and socio-economic conditions that collectively facilitate online commercial transactions. It has grown rapidly due to increased internet penetration, smartphone adoption, and the proliferation of digital payment solutions.[46]

However, at the core of Nigeria's e-commerce ecosystem are key stakeholders including online retailers, logistics providers, payment solution vendors, telecommunications companies, government regulators, and consumers. Together, these stakeholders shape the functionality and competitiveness of the e-commerce market. Digital platforms such as Jumia, Konga, and local marketplaces have gained prominence by offering diverse products and services, yet they operate within a challenging environment defined by inconsistent logistics networks and high transaction costs.[47]

---

[42] D Wall, (n33)

[43] Cybercrime (Prohibition, Prevention, etc.) Act 2015 (as amended 2024), s6

[44] Ibid, s11

[45] Evidence Act 2011 (as amended 2023), s84

[46] S Adeoye & O Elegunde, 'E-Commerce Adoption in Nigeria: A Strategic Imperative for Service Organizations' *International Journal of Academic Research in Business and Social Sciences* [2012] 3(3) 289-301

[47] L Chinomona & M Sandada, 'The Influence of E-Commerce Adoption on Organisational Performance' *Mediterranean Journal of Social Sciences* [2013] 5(2) 459-468

A critical component of this is the digital payment infrastructure, which enables the execution of monetary transactions online. Mobile money services, bank card systems, and fintech solutions are expanding access to digital payments, particularly among previously unbanked populations. Nevertheless, trust deficits arising from fraud, weak authentication, and data breaches have slowed the widespread adoption of online payment channels.[48]

Regulatory and institutional frameworks also influence ecosystem development. Policies such as the Nigeria Data Protection Regulation (NDPR) and the Cybercrimes Act aim to provide legal safeguards for data privacy and electronic offenses, yet enforcement challenges persist (NITDA 2019; Cybercrimes Act 2015 (as amended) 2024) which are essential for promoting consumer protection, enhancing system credibility, and attracting foreign and domestic investment into the e-commerce sector.[49]

Socio-economic factors, including population demographics, income levels, and digital literacy, further shape the dynamics of Nigeria's e-commerce ecosystem. With a predominantly young population and rising internet usage, the potential demand for online goods and services is substantial. However, disparities in access to digital skills and infrastructural resources create uneven participation across regions and socio-economic groups.

## 2.5 Cyber Insurance

Romanosky defined cyber insurance as a range of expenses including legal fees, notification fees, public relation efforts, and even ransom payments, providing critical financial support in the

---

[48] O Ogunlowo & S Ikhide, 'Trust and Consumer Purchase Intention in Nigerian E-Commerce'
*Journal of Internet Commerce* [2019](14)4) 312-330

[49] Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended) 2024, s14-23; Nigerian Communications Commission, Consumer Code of Practice Regulations 2007, reg 32-35

aftermaths of cyberattacks.[50] Cyber insurance is a type of insurance policy designed to help organizations mitigate financial losses resulting from cyber incidents like data breaches, ransomware attacks, or business interruptions caused by cyber threats. As a specialized policy is a strategic shield against cybercrime and espionage is to mitigate loses arising data breaches, ransomware attacks, cyber espionage, and business disruptions which are key threats to digital enterprise and e-commerce platforms.[51] Benefits of cyber insurance as stated by ENISA is that it helps organizations recover financially from cyber incidents, encourages companies to cybersecurity measures, provides access to expert resources and supports regulatory compliance.[52]

## 3. Legal Framework

The key legal frameworks relevant to this paper include:

### 3.1 The Constitution of the Federal Republic of Nigeria, 1999 (as amended 2023)

The Constitution of the Federal Republic of Nigeria serving as the ultimate reference point for all laws,[53] remains the supreme law of the land[54] which is binding on all persons and authorities within Nigeria.[55] Since cybercrime involves national security, international cooperation, and cross-border issues, the National Assembly has clear constitutional backing to enact laws to promote cybersecurity like the Cybercrime Act 2015 and others.[56] Also, the exclusive list

---

[50] S Romanosky, 'Examining the Cost and Causes of Cyber Incidents' *Journal of Cybersecurity* [2016] (2)(2) 121-135

[51] J P Kesan & C Hayes 'Mitigate Countermeasures: Cybersecurity Insurance and Its Influence on Security Investment' *Journal of Law, Technology & Policy* [2017](2)(1) 211-247

[52] ENISA, *Cyber Insurance Challenges, Trends and Practices* (18th February, 2020) available @ <https://www.enisa.europa.eu/publication/cyber-insurance-challenges-trends-and-practice> accessed on 19th October, 2025

[53] E Ojo, *Constitutional Law in Nigeria* (Ibadan: Spectrum Books Ltd 2019) 14

[54] CRFN 1999, s1(1)

[55] Ibid, s1(3)

[56] Ibid, s4(2)

empowers the national assembly to make laws to promote and enforce the observance of fundamental objectives and Directive Principles of State Policy.[57]

The Act made provision for right to private and family life also known as right to privacy which safeguards citizens from unauthorized surveillance, data collection, or communications interception unless done under legally;[58] right to freedom of expression and the press[59] endorsed by a landmark case *Arthur Nwankwo v. The State*[60] remains an authority of online expression, particularly where individuals use digital platforms to voice dissent or criticize government policy is constitutionally protected unless they cross the threshold into criminal conduct like incitement or hate speech; restriction on and derogation from fundamental human rights recognizes that fundamental rights can be lawfully restricted in the interest of public order, safety, or morality, but restrictions must be reasonably justified in a democratic society;[61] right to fair hearing[62] within a reasonable time and presumption of innocence[63] is the bedrock for an unbiased judgment to be laid. *Deduwa & Ors v. Okorodudu*[64] the Supreme Court emphasized that a fair hearing meant that parties must be given equal opportunity such as timely notice, representation by counsel, and access to evidence to present their case before an impartial tribunal.

Likewise, the Constitution mandates that government appointments and operations reflect Nigeria's ethnic and regional diversity to promote national unity and inclusiveness[65] which guides the

---

[57] Ibid, Second Schedule, Part I, 60 & 68
[58] CRFN 1999, s37
[59] Ibid s39(1)
[60] (1985) 6 NCLR 228
[61] CRFN 1999, s45(1)
[62] CRFN 1999, s36(1)
[63] Ibid, s36(5)
[64] (1976) 9–10 SC 329
[65] CRFN 1999, s14[3]

composition and cooperation of agencies responsible for cybercrime enforcement such as the Economic and Financial Crimes Commission (EFCC), Nigerian Police Force (NPF), and Nigerian Communications Commission (NCC) which was further stressed in *Attorney-General of the Federation v. Abubakar*.[66]

### 3.2 Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024)

This Nigeria's principal legislation first enacted in 2015 and amended in 2024 aimed at combating cyber threats and offences while playing a critical role in regulating digital conduct, protecting computer systems, and ensuring the integrity of online platforms.[67] Some provisions are particularly relevant to cyber espionage which involves illicitly obtaining proprietary or sensitive information through hacking or data infringements.[68] They include: unauthorized access to computer systems,[69] forgery of electronic documents (used in falsifying authentication),[70] and system interference.[71] The act went further to criminalize key cyber threats like phishing, card fraud, online scams, and others which are classified as identity theft and impersonation,[72] cyberstalking and cyberbullying mostly e-commerce merchants,[73] electronic card fraud,[74] and use of fraudulent devices or access codes.[75] By this Act, provisions were made to empowers law enforcement agencies to

---

[66] (2007) 10 NWLR (Pt. 1041) 1 (SC)

[67] U Okoro, & A Chined, 'Legal Responses to Cyber Espionage in Nigeria's Digital Economy' *African Journal of Law and Technology* [2021](6)(3) 75-90

[68] O Adereti & A Musa, 'Cybersecurity & Ecommerce in Nigeria: Legal and Institutional Framework' *Journal of African Law and Technology* [2020](5)(2) 123-140

[69] Cybercrimes (Prohibition, Prevention, etc) Act, 2015 (as amended 2024), s6

[70] Ibid, s8

[71] Ibid, s12

[72] Ibid, s14(2)

[73] Ibid, s13

[74] Ibid, s15

[75] Ibid, s17

investigate and prosecute cybercrime,[76] and requires service providers to cooperate with investigations.[77]

### 3.3 Nigeria Data Protection Regulation, 2019

The Nigeria Data Protection Regulation (NDPR) was promulgated in 2019 after the General Data Protection Regulation (GDPR) 2018 by the National Information Technology Development Agency (NITDA) governs data protection and privacy which marks a pivotal advancement in Nigeria's efforts to enhance data protection and combat cybercrime. The Acts sole aim is to: protect personal data ensuring that data is processed lawfully, fairly and transparently[78] which requires organizations to obtain explicit consent and process data in compliance with legal principles;[79] enhance data security to safeguards to protect personal data and prevent unauthorized access, loss, or alteration of data;[80] cultivate consumer confidence in digital platforms[81] while ensuring transparency and empower data subjects;[82] implement mechanisms for monitoring adherence to data protection principles and enforcing sanctions for violations.[83] Provisions were also made to address cyber espionage and cybercrime, posing significant threats to e-commerce growth such as: awareness of data breach must be notified within 72hrs enabling rapid response to mitigate harm from cyberattacks;[84] imposing stringent obligations and security frameworks protects against unauthorized access to data;[85] overseeing compliance and risk

[76] Ibid, s41-46
[77] Ibid, s38-s40
[78] NDPR 2019, s3
[79] Ibid, s4
[80] Ibid, s7
[81] Ibid, s9
[82] Ibid, s10
[83] Ibid, s23
[84] Ibid, s15
[85] Ibid, s7

management should be done by data protection officer;[86] cross-border data transfer must be of standards;[87] and provides penalties like fines based on gross annual revenue, to deter non-compliance and negligent practices that could facilitate cybercrime.[88]

### 3.4 Nigeria Data Protection Act, 2023

The Nigeria Data Protection Act (NDPA) 2023 is a landmark legislative development established by the Nigeria Data Protection Commission (NDPC), a regulatory body with the authority to supervise and enforce data protection compliance.[89] A major impact of the NDPA on cybercrime prevention is that it grants these consumers several rights, including the right to be informed, the right of access, the right to rectification, the right to erasure, and the right to data portability.[90] Under the act, entities can determine the purpose of data processing (controllers) and those that process data on their behalf (processors) are obligated to implement appropriate technical and organisational measures to ensure data security.[91] In situations of data breach there should be a prompt notification of the affected individuals and the NDPA which would enable parties to take precautionary steps such as freezing accounts or changing passwords while also empowering regulators to investigate the cause and scale of the breach.[92] The Act further contains specific provisions aimed at regulating cross-border data transfers involving cloud-based services or international payment processors.[93]

---

[86] Ibid, s14
[87] Ibid, s21
[88] Ibid, s23
[89] NPDA 2023, s5-s11
[90] Ibid, s24-s31
[91] Ibid, s39
[92] Ibid, s40
[93] Ibid, s44-s46

### 3.5 Evidence Act 2011 (As amended 2023)

The Evidence Act, 2011 is the principal legislation governing the admissibility, relevance, and weight of evidence in Nigerian courts but it was amended 2023 to modernize rules on electronic evidence, digital signatures, certification of electronic records, and burden of proof. The act laid down the principle of relevance and admissibility,[94] conditions for the relevance of fact,[95] types of evidence which could be documentary evidence,[96] primary or secondary evidence,[97] the conditions for admitting, and the special rules around secondary evidence.[98] Moreso, the main purpose of the amendment of the act especially for cybercrimes, e-commerce, digital communication, and technology-based cases by laying the principle of admissibility of electronic (computer-based) evidence including emails, call logs, CCTV footage, phone messages, bank records, online transactions records, computer files, and many more.[99] It further emphasized that courts must take judicial notice of laws, official gazettes, signatures of public officers[100] and gave a modernized definition for computer, electronic record, documents, electronic signature, digital records, and others.[101]

## 4. Consumer Trust and the Role of Digital Forensic in Securing Nigeria's E-Commerce System

In this section**,** there would be an in-depth analysis on the topic of this paper.

---

[94] EA 2023, s1 & s3
[95] Ibid, s4-s14
[96] Ibid, s85-s87
[97] Ibid, s89
[98] Ibid, s90
[99] Ibid, s84
[100] Ibid, s122
[101] Ibid, s258

### 4.1 Overview of Nigeria's E-Commerce Landscape

Nigeria's e-commerce sector has experienced rapid expansion in recent years, fueled by rising internet penetration, smartphone adoption, expanding digital payment solutions, and a growing youthful population. In 2025, the e-commerce market in Nigeria was valued at around USD 9.35 billion, with projections showing robust growth through the end of the decade, potentially reaching approximately USD 17 billion by 2030 as online retail continues to scale.[102]

The growth of e-commerce in Nigeria is underpinned by several structural and demographic trends: mobile internet and device usage with over 141 million mobile internet subscribers, the market is increasingly mobile-first, as consumers prefer shopping on smartphones, young, tech-savvy population which is a growing population of internet users estimated at over 100 million has expanded the pool of potential online buyers and encouraged platforms to innovate.[103] Urban demand from cities like Lagos, Abuja, and Port Harcourt dominate e-commerce activity due to better infrastructure and higher broadband coverage, capturing a large share of online orders has encouraged both established marketplaces and emerging players to expand product offerings, enhance logistics, and tailor services to local preferences.[104]

Again, Nigeria's e-commerce ecosystem is populated by both local and international platforms. Jumia remains one of the most recognized e-commerce marketplaces, leading in order volumes and continued expansion efforts.[105] Other platforms such as Konga,

---

[102] C Michael, 'Nigeria's E-Commerce Transactions to Reach $33bn By 2026' *BusinessDay* (Lagos:17th January, 2025)

[103] T Ojo, 'Nigeria: An Analysis of Payments and E-Commerce Trends' *Jumia Group* (Lagos: 4th November 2025)

[104] C Okereocha, Fierce Competition for Nigeria's $9.54 Billion E-Commerce Market' *The Nation* (Lagos, 21st January 2025)

[105] A Atogebania, 'Nigeria's E-commerce Market Expected to Hit $33 Billion by 2026' *Managing Nigeria* (Lagos, 26 April 2025)

Ajebo Market, Slot, DealDey, PayPorte, and Kilimall represent diverse niches in fashion, electronics, deals, and lifestyle products. Also, social commerce has also become a vital channel, with many micro‑businesses selling directly to consumers through Instagram, WhatsApp, and Facebook, reflecting the market's grassroots adoption patterns.[106]

Furthermore, payment methods are evolving but still hybrid. While digital payment adoption is growing, cash‑on‑delivery continues to account for a significant share of transactions reflecting persistent trust and infrastructure challenges in online payment systems. Fintech firms and mobile wallet services (e.g., Paystack, Flutterwave, JumiaPay, Paga) are driving innovations in digital payments, enhancing convenience and security for online buyers. Mobile money agents and USSD channels are helping bridge gaps for customers without consistent internet or banking access, supporting financial inclusion.[107]

Despite strong growth momentum, Nigeria's e‑commerce ecosystem faces significant headwinds of infrastructure gaps like road networks, unreliable electricity, and underdeveloped delivery systems contribute to high logistics costs and slower delivery times outside major urban centres, payment trust issues as many consumers remain cautious about sharing financial information online due to fraud risks, reinforcing reliance on offline payment alternatives, digital divide which vary internet quality and digital literacy, especially in rural areas, limit the pace of digital adoption across the country, consumer trust deficits over product quality, returns, and secured transactions.[108]

---

[106]Go-Globe, *E□Commerce In Nigeria: Growth And Future Trends 2024* (Lagos: 19th February, 2025) available @ ≤https://www.go-globe.com/e-commerce-in-nigeria-growth-and-future-trends> accessed on the 25th December, 2025

[107] T Ojo, (n100)

[108] C Okereocha, (n101)

Looking ahead, Nigeria's e-commerce sector is expected to sustain strong growth, supported by broader digital transformation and economic shifts. Expansion beyond traditional hubs into secondary cities and rural markets will hinge on better infrastructure, logistics innovation, and cross-sector collaboration as digital payments, regulatory frameworks, and consumer confidence mature, e-commerce adoption is likely to deepen, attracting more investment and competitive entry.[109]

### 4.2 Consumer Trust and Challenges in Nigeria's E-Commerce Sector

Consumer trust is widely recognised as a critical determinant of e-commerce adoption because, unlike traditional retail, online shopping involves remote transactions without physical interaction between buyers and goods. In Nigeria, trust challenges significantly hinder the growth of online shopping, shaping how consumers evaluate risk, make purchase decisions, and choose payment methods.[110]

A major obstacle in Nigeria's e-commerce sector is the widespread perception of risk, especially concerning online security and fraud. Consumers frequently worry that their personal and financial information could be stolen or misused, which discourages them from completing online transactions.[111] This apprehension is intensified by recurrent reports of phishing attacks, data breaches, and cyber fraud, which erode trust in digital payment systems and online platforms. As Nwankwo highlights, the inconsistent application of cybersecurity protocols and varying standards across

---

[109] E Ade, 'Nigeria's E□Commerce Market Set To Surpass $16 Billion By 2030, Fueled by Jumia, Konga, and Digital Innovation' *Market News Nigeria* (Lagos, 22nd September 2025)

[110] G T Abraham, E F Osaisai, N S Dienagha & A Ineyekineye, 'Usability, Security and Trust of E□Commerce Websites: The Effect on the Nigerian E□Shopper' *Asian Journal of Research in Computer Science* [2021](10)(4) 58-68

[111] S Akinyele & O Olumide, 'Cybersecurity Threats and Consumer Confidence in Nigerian E-Commerce' *Nigerian Journal of Cybersecurity* [2020](3)(2) 50-65

different e-commerce platforms create a fragmented security environment. This lack of a unified security framework discourages consumer participation and hampers the growth of online commerce in Nigeria.[112]

Moreover, weak enforcement, low consumer awareness and fragmented regulations across sectors exacerbates trust issues. Many Nigerian consumers are skeptical about the reliability of online vendors due to a history of fraud, counterfeit products, and delayed or non-delivery of goods. This skepticism often leads to a preference for cash payments upon delivery, which, while perceived as safer, limits the growth of digital payment adoption. As Aker emphasizes, the absence of effective regulatory enforcement and consumer protection laws creates an environment where consumers feel vulnerable and less willing to engage fully with e-commerce platforms.[113]

Another significant barrier is the limited digital literacy among a substantial portion of the population. Many consumers lack sufficient understanding of digital payment systems and online transaction processes, which heightens perceived risks and discourages online shopping.[114] This digital divide not only hampers trust but also restricts the broader inclusion of marginalized groups into the e-commerce ecosystem.

Furthermore, infrastructural challenges such as unreliable internet connectivity and inconsistent electricity supply undermine consumer confidence in the stability and security of online platforms. These infrastructural deficits lead to fears about

---

[112] C Nwankwo, 'Infrastructural Challenges and the Growth of E-Commerce in Nigeria' *African Journal of Information Systems* [2019](11)(3) 45-60

[113] J Aker, 'E-Commerce and Consumer Protection in Nigeria' *Nigerian Economic Review* (Lagos: 4th July, 2021) 15-30

[114] T Olaleye, 'Digital Literacy and E-Commerce Adoption in Nigeria' *International Journal of Digital Economy* [2020](4)(2) 78-92

transaction failures and data loss, further dampening trust in the e-commerce sector.[115]

To address these trust challenges, stakeholders including government, e-commerce firms, and financial institutions must collaborate to implement stronger cybersecurity measures, enforce consumer protection laws, and promote digital literacy. Building consumer confidence is essential for fostering sustainable growth and expanding the reach of e-commerce in Nigeria.[116]

### 4.3 Digital Forensics as a Tool for Securing E-Commerce Platforms

Digital forensics is the systematic discipline of identifying, preserving, analyzing, and presenting digital evidence from electronic devices, networks, or online platforms.[117] It is a key mechanism in securing e-commerce platforms against cybercrime, ensuring consumer trust, and supporting compliance with legal and regulatory frameworks.[118] For Nigeria, integrating forensic practices is crucial for protecting sensitive customer data, financial transactions, and business reputations.

This emphasizes that the role of digital forensics is to help detect patterns of fraud in real time by monitoring transactional data, user behaviors, and network activity with forensic tools which can identify unauthorized access, phishing attacks, fake listings, and compromised accounts;[119] enable the investigation of breaches,

---

[115] C Umeh, 'Cybersecurity and Trust in Nigerian E-Commerce' *Nigerian Journal of Cybersecurity* [2023](2)(1) 10-25

[116] M Ibrahim, 'Security Challenges and Consumer Confidence in Nigerian Online Markets' *Journal of Digital Commerce* [2024](5)(1) 33-47

[117] E Cassey, (n28)

[118] S Raghavan & S Bhattacharya, Digital Forensics: Principles and Practices (1st edn; New York: Springer, 2020) 5

[119] P Kaur & A Chhabra, 'Role of Digital Forensics in Cybersecurity for E□Commerce Platforms' *International Journal of Computer Applications* [2021](176)(14) 15-22

identification of vulnerabilities, recovery of data, and reconstruction of attack timelines and due compliance with Nigeria's Data Protection Act 2023 to ensure that forensic investigations align with data privacy laws;[120] insights from forensic investigations help e-commerce operators enhance their cybersecurity posture by understanding attack vectors and implementing measures such as multi-factor authentication, enhanced encryption, intrusion detection systems, and regular vulnerability assessments, reducing the risk of future incidents;[121] provide admissible evidence for prosecuting cybercriminals under Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended) 2024 and the Evidence Act 2011 (as amended 2023) and pursue legal action, recover losses, and reinforce the deterrent against cybercrime;[122] enhance consumer trust mostly to e-commerce platforms implementing forensic monitoring and incident response frameworks;[123] and it ensures compliance with national and international cybersecurity and data protection standards, including Nigeria's Data Protection Act 2023, ISO/IEC 27001, and PCI DSS. Besides, there are several branches of digital forensics employed to extract and preserve evidence without compromising its integrity such as: email and log analysis traces phishing campaigns, suspicious logins, and social engineering attacks; network forensic monitors and analyzes network traffic to detect intrusions, malware communication, and unusual activity patterns; mobile device forensics investigates mobile app usage, detecting unauthorized access to wallets or apps, and monitoring app-level vulnerabilities;

---

[120] T Owolabi, A Ojo & K Adewale, 'Digital Forensics and Data Protection in Nigerian E-Commerce' *Nigerian Journal of ICT and Digital Economy* [2023](12)(1) 33-48

[121] M Ahmad, S Abdullah, & F Malik, 'Cyber Forensics Framework for Securing E-Commerce Transactions' *Journal of Cybersecurity Research* [2021](5)(2) 45-60

[122] B Umar, & F Akinsola, 'Legal Admissibility of Digital Evidence in Nigerian Cybercrime Cases' *African Journal of Law and Technology* [2022](9)(3) 67-82

[123] S Adeyemi & T Olaniyi, (n18)

database forensics examines database logs and transaction histories for tampering, unauthorized modifications, or anomalies; cloud forensics analyzes cloud-stored data, such as payment histories, product inventories, and user data, for breaches or tampering; AI-assisted forensics uses machine learning to predict anomalies, detect fraud, and automate forensic analysis, improving speed and accuracy.[124]

Similarly, emerging branches and techniques of digital forensics relevant to e-commerce growth are: blockchain forensics helps ensure transparency and traceability in cryptocurrency transactions on e-commerce platforms; AI-driven anomaly detection automates identification of suspicious patterns and potential fraud in real time; integration with SIEM (Security Information and Event Management) centralizes logging and monitoring to detect threats quickly and cross-border forensic frameworks which addresses challenges of multi-jurisdictional investigations, crucial for international e-commerce platforms.[125]

Although, digital forensic is very pivotal to the growth of e-commerce in Nigeria, it suffer challenges of implementation as there is limited availability of trained forensic investigators with expertise in cybercrime, the cost of forensic tools, software, and infrastructure are often expensive, cybercriminals adopt new attack vectors which requires the constant forensic update, regulatory compliance of forensic investigation respecting data protection laws to avoid legal liabilities, and inconsistent internet and power infrastructure affect timely forensic investigations.[126]

---

[124] K Jones & R Valli, (n29)

[125] E E M Micah, I H Saidu, T Ibitomi & B S Sanusi, (n15)

[126] V Ishaya, (n16)

Digital forensics secures e-commerce platform in the following ways

i. It allows specialist to trace fraudulent transactions, identify attackers and assist with legal proceedings.
ii. It analyses network traffic and system log by identifying anomalies that indicate potential threats before they cause significant damage.
iii. It ensures that digital evidence such as logs, transaction are properly collected and maintained, which is crucial for legal actions and maintaining consumer trust.
iv. It helps detect malicious activities from unauthorized access by employees within.

Digital forensics is no longer optional but a critical component of e-commerce security in Nigeria and by integrating modern forensic tools, AI-assisted analysis and threat detection, and international best practices Nigeria's e-commerce ecosystem is further secured against the rising tide of cyber threats and helps maintain compliance with regulations.

## 5. Conclusion and Recommendations

Digital forensics is an indispensable component of e-commerce security in Nigeria. It enables the detection and prevention of fraud, investigation of data breaches, legal evidence collection, and regulatory compliance, all of which contribute to enhancing consumer trust. Nigeria is institutionalizing the link between forensics and trust by shifting from paper-based oversight to science-based governance. The National Digital Trustmark is a verifiable certification badge designed for e-commerce platforms in Nigeria, launched by the National Information Technology Development Agency (NITDA). It acts as a security seal to confirm legitimate businesses, fight online fraud, and boost consumer confidence in digital transactions

Despite challenges such as limited forensic expertise, high implementation costs, and rapidly evolving cyber threats, adopting a comprehensive forensic framework can significantly strengthen the resilience and credibility of Nigerian e-commerce platforms by integrating advanced forensic tools, regulatory compliance, consumer education, and multi-stakeholder collaboration, Nigerian e-commerce firms can build secure, trustworthy, and sustainable digital marketplaces, fostering growth in online transactions and supporting the country's digital economy.

The following recommendations are hereunder made:

1. To encourage Nigerian e-commerce firms to invest in training and certification programs for IT staff in digital forensics and cybersecurity. Also, partnership with universities and professional bodies can develop specialized programs that equip personnel with skills in network, database, cloud, and mobile forensics.
2. To adopt advanced forensic tools like AI-powered forensic tools, Security Information and Event Management (SIEM) systems, and blockchain monitoring solutions which automate anomaly detection, fraud tracing, and incident investigation, reducing response time and improving accuracy.
3. To ensure that forensic investigations are aligned with Nigeria's Data Protection Act 2023, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024), and international standards such as ISO/IEC 27001 which guarantees legal compliance, protects consumer rights, and enhances trust.
4. To educate consumers on safe online practices, signs of fraud, and steps to take in case of breaches and this reduces susceptibility to cybercrime and strengthens consumer confidence in Nigerian e-commerce.
5. To collaborate among e-commerce firms, law enforcement, financial institutions, and cybersecurity experts as shared

intelligence on cyber threats can improve response time and preventive measures, creating a safer e-commerce ecosystem.

6. To conduct periodic vulnerability assessments, penetration testing, and forensic readiness audits and this ensures that systems are prepared to collect, preserve, and analyze digital evidence effectively when incidents occur.
7. Rebuilding trust by a long term commitment to security and proactive remediation.