ELECTRONIC SIGNATURES AND ELECTRONIC CONTRACTS UNDER NIGERIAN LAW: LEGAL VALIDITY, EVIDENTIAL CHALLENGES AND FUTURE PROSPECTS

Majebi Samuel Amune*

Abstract

The fast development of information and communication technologies has greatly changed how business transactions are conducted, leading to the wide use of electronic signatures and electronic contracts with great benefits. However, even with these benefits, there are still legal uncertainties and practical difficulties regarding the legality, evidence, and enforceability of electronic signatures and contracts. This paper examined the legal rules that apply to electronic signatures and contracts in Nigeria, with a focus on their validity, the challenges in proving them, and their future potential. The paper adopts doctrinal approach. A comparison with international standards is also used to assess how Nigeria is performing against global best practices. The paper finds that although Nigerian law acknowledges electronic signatures and contracts, there are still major challenges that prevent them from being fully effective. The paper suggests the need for clearer laws on electronic authentication, better training for judges on digital evidence among others

* LL.B. (University of Benin); LL.M., M.Phil., PhD (Obafemi Awolowo University) Senior Lecturer, College of Law, Joseph Ayo Babalola University, Ilesa, Osun State, Nigeria & Principal Partner, LawDigital Consult. Email: nobleheirs@yahoo.com

Keywords: Electronic Contract, Electronic Signature, E-Commerce, Evidence Act 2011, NITDA

1.0 INTRODUCTION

Digital evolution sparks a transformative shift as virtually everything traditionally conducted through a physical means can be executed electronically easily, effectively and efficiently. Forming the cornerstone of the foregoing is the means of contracting. The growth of electronic contract is mediated by several factors including the widespread adoption of mobile phones and other telecommunication systems, predominance of digital payment systems, and particularly the increased growth of electronic commerce platforms. This form of contract presents innovative and groundbreaking benefits spotlighting a justification for the switch in the conventional paper and pen contract to the digital means of contracting.

Viewed from this background, the transformation is not limited to the means of contract, as the revolution is furthered to the expression of consent, essentially introducing the electronic signature. This form of signature brings convenience and ease, eliminating the need for a physical presence in appending signatures to a document attributed to the traditional signature.

Despite the preponderance of benefits embedded in the electronic form of contracting and appending signatures, the forms taken by these two have outpaced the existing regulatory frameworks, creating substantial element of security and legitimacy doubts. This challenge is furthered by the pseudonymous nature of the internet, shielding the identity of individuals behind legally binding agreements.

Against this backdrop, this work starts by examining electronic contracts, and *inter alia,* electronic signatures. It furthers to identifying the different forms of electronic contracts *vis-á-vis* the conventional contracts. Additionally, it analyses the key legal frameworks governing electronic contracts and electronic signatures in Nigeria, while evaluating the legislative gaps gleanable from these frameworks. Ultimately, it examines different spheres to serve as a guide in making critical and pivotal suggestions for creating a balance between ensuring innovations and capture the prospective challenges posed by digital contracts and signatures.

2.0 CONCEPTUAL AND THEORETICAL FRAMEWORK

Before furthering the discourse of this work, it is critical to conceptually clarify the key words theoretically employed in this work. Subsequently, this section is dedicated to look into these key terms, and the manner in which they have been contextualised to form the central idea of the work.

2.1 Meaning and types of electronic signatures

The world is on a digital shift, justifying why a document may be signed electronically. An electronic signature is the electronic version of the traditional signature which is usually handwritten.[1] In a simple form, electronic signature is identified as e-signature and is seen as a method by which a document is digitally signed.[2] Pertinent it is to say, while this form of signature is often identified to mean a digital signature, they are

[1] Rahul Awati, 'e-signature (electronic signature)' (T*echtarget,* 2023) available at https://www.techtarget.com/searchcontentmanagement/definition/e-signature accessed 23 January, 2026.

[2] Yasamin Yousefi, 'What is an Electronic Signature?' (*docusign,* 2023) available at https://www.docusign.com/blog/what-electronic-signature accessed 23 January, 2026.

distinct, and are not usable interchangeably.[3] Resultantly, all digital signatures are electronic signatures, but not all electronic signatures are digital signatures.[4]

2.2 Concept and forms of electronic contracts (click-wrap, browse-wrap, shrink-wrap

Unlike the traditional contract which usually requires a physical presence before it is formulated, electronic contract is a legally binding agreement conducted and formulated through the use of an internet.[5] Parties to this contract usually enter into this agreement through a digital means without a physical interactions as it is drafted, negotiated, offered, accepted and

[3] As established in the body of the work, an electronic signature is a fast, simple and efficient way of signing a digital document in the same manner in which a physical document would be signed conventionally. A digital signature on its part is a form of signature that makes use of cryptography in signing an electronic document, and this is usually more secure. Unlike an electronic signature which may be a mere signature, or a scanned signature or the click of an agree button, this signature makes use of public cryptography and ensures 3 key things – authentication, by confirming the identity of the signer; integrity, by ensuring that the document is no altered, and in the event of an alteration, it is indicated. Thirdly, it ensures that the signer cannot deny signing the document, as their identity verifiable through digital certificate containing information about the person is made known, therefore eliminating all possibility of denials. More can be explored about the differences between the two at https://www.geeksforgeeks.org/computer-networks/difference-between-electronic-signature-and-digital-signature/ accessed 23 January, 2026.

[4] Electronic signature represents the general name for all signatures signed digitally, which include scanned signatures, the click to agree signatures, and digital signatures themselves. Digital signature on the flip side is just a form of electronic signature distinct to other forms of electronic signatures.

[5] Ironclad, 'What Is an Electronic Contract?' (*Ironclad,* 2024) available at https://ironcladapp.com/journal/contracts/what-is-an-electronic-contract accessed 23 January, 2026.

executed online.[6] As long as the essential elements of a valid contract subsist, the validity and enforceability of this contract are not impaired.[7]

2.2.1 Forms of Electronic Contracts

i. Click-wrap

Also known as click-through agreement.[8] It is often the most commonly seen agreement, and it occurs when an individual has to agree to the terms and conditions of a website or a software before use or download. Before advancing, the person intending to make use of the website has to click an "I agree" or "I accept" button.[9] Instead of having to make every user assent to the terms by signing a digital document, the individual merely has to click a checkbox or a button indicating his consent, hence the derived named, 'click-wrap'.[10]

---

[6] Ibid.

[7] LawTeacher, 'Electronic Contracts' (*LawTeacher,* 2018) available at https://www.lawteacher.net/free-law-essays/contract-law/electronic-contracts.php#citethis accessed 23 January, 2026.

[8] 'Clickwrap Agreement' (*Thomas Reuters*) available at https://uk.practicallaw.thomsonreuters.com/8-511-1310?transitionType=Default&contextData=(sc.Default) accessed 24 January, 2026.

[9] Sharon Shea, 'click-wrap agreement (click-through agreement)' (*Techtarget*, 2024) available at https://www.techtarget.com/searchcloudcomputing/definition/clickwrap-agreement-clickthrough-agreement accessed 24 January, 2026.

[10] Francis M. Buono and Jonathan A. Friedman, 'Maximizing the Enforceability of Click-Wrap Agreements' (1999) 4(3) article 4 *Journal of Technology Law & Policy* available at <http://journal.law.ufl.edu/-techlaw/4-3/friedman.html?> accessed 24 January, 2026.

ii. Shrink-Wrap

This is an agreement where the terms and conditions of a product are made available only after the product package or seal is broken.[11] Unlike a click-wrap agreement where a user has the opportunity to read through the terms and conditions of a website or software before assenting, a shrink-wrap agreement is largely characterised by implied consent, owing to the fact that the terms and conditions in a shrink-wrap agreement are enclosed within the product's packaging.[12]

iii. Browse-wrap

This is usually used on websites. It is an agreement where a site owner implies consent by asserting that a user's continuous use of the website indicates the person's acceptance of the terms and conditions as well as the privacy policy of the site.[13] Unlike a click-wrap which requires a user to click the accept button, the assent here is implied, and a user's continuous stay on a website is deemed to be his acceptance of the terms of the website.[14]

---

[11] Nicolas and De Vega Law Offices, 'Shrink-Wrap Agreements: Are They Valid Contracts?' available at https://ndvlaw.com/shrink-wrap-agreements-are-they-valid-contracts/ accessed 24 January, 2026.

[12] Ruchika Bhatt & Hiteashi Desai, 'Shrink Wrap & Click Wrap Agreements and their Enforceability in India' (*Lexology,* 2025) available at https://www.lexology.com/library/detail.aspx?g=f254d166-17ca-477f-a0fc-97d5ddc3bb8b accessed 24 January, 2026.

[13] Natasha Piirainen, 'Clickwrap vs. Browsewrap Agreements and When To Use Them' (*Termly,* 2026) available at https://termly.io/resources/articles/browsewrap-vs-clickwrap/ accessed 24 January, 2026.

[14] Ibid.

2.3 Distinction between electronic and traditional contracts

The first distinction between the two contracts lies in their accessibilities. A traditional contract requires a physical document before it could be accessed, and except where it is laid, a physical document containing the terms of a contract cannot be accessed anywhere. On the other hand, an electronic contract can be accessed anywhere, as long as there is an internet connection to do so. This makes an electronic contract easily accessed and faster.[15]

Additionally, a traditional contract is vulnerable to physical damage, theft or forgery, while an electronic contract makes use of digital security, encryption and digital signatures giving it a robust level of security against forgery, or unauthorised access.[16]

Traditional contract attracts higher cost, due to the cost associated with the printing of papers, system of arranging terms of a contract, and a physical storage to keep paper terms. Conversely, electronic contract does not require much of these before serving its purpose, as it adopts a cloud-based storage, significantly reducing the costs which may come with a traditional contract.[17]

---

[15] Mostafa Elsaied, 'Electronic contracts vs. traditional contracts: A handy comparison' (*Oneflow,* 2024) available at https://oneflow.com/blog/traditional-contracts/ accessed 24 January, 2026.

[16] 'E-contracts vs traditional contracts: modernizing agreements' (*Enty,* 2024) available at https://enty.io/blog/econtracts-vs-traditional-contracts accessed 24 January, 2026.

[17] Dottedsign Team, 'Electronic Contracts vs Traditional Contracts: An In-Depth Analysis' (*Dottedsign*, 2024) available at https://www.dottedsign.com/blog/product/electronic-contracts-vs-traditional-contracts accessed 24 January, 2026.

2.4 Principle of consent and intention in electronic transactions

At the heart of contract law lies the requirement that an agreement entered into between parties must have stemmed from meeting of the minds, which is their consent, and parties' intent to be bound by the agreement entered into. While an electronic contract may have taken a different form, it serves the same purpose with a traditional contract, predicated on that they both serve as an avenue for parties to impose duties and obligations on each other.

Viewed from this background, it is accordingly placed that electronic transactions do not challenge the very notion of consent and intention under contract law. Applying the theories of contract law to electronic transactions, while the form in which consent and intention manifest may differ, the underlying legal effect remains the same. The click of accept button is deemed an acceptance under a click-wrap agreement; a further engagement with a website is deemed the expression of consent under a browse-wrap agreement; and the opening and installing of a software package is deemed as a form of consent under the shrink-wrap contract. In view of the foregoing, intentions is distillable from electronic transactions through a user's submission of personal data, completion of transactional steps among many others. This is contingent upon the fact that all these cannot presumably be done by a person mindlessly or in an unfit mental state.

3.0 LEGAL FRAMEWORK GOVERNING ELECTRONIC SIGNATURES AND ELECTRONIC CONTRACTS IN NIGERIA

3.1 Constitutional Basis for Electronic Transactions

The 1999 Constitution of the Federal Republic of Nigeria is the supreme document of the land,[18] establishing government powers, and dividing those powers within different levels and organs of government. This document is supreme, and its provisions are binding on all authorities and persons throughout Nigeria.[19] In any situation where any law goes against the provision of the Constitution, to the extent of its inconsistency is the voidness and nullification of such a law.[20]

While the Constitution has not expressly provided for electronic transactions, the legal validity is derived from the establishment of national bodies, and the powers granted to the branches of government to establish bodies and legal frameworks that establish electronic transactions and give it the same status as a traditional paper-based agreement.

3.2 The Evidence Act 2011 and Electronic Signature

3.2.1 The Evidence Act 2011

One of the foremost legal frameworks regulating electronic contract and electronic signature in Nigeria is the *Evidence Act*. The Act was enacted in 2011 to repeal the *Evidence Act, 2004* and to serve as the primary law providing the guide on the use and submission of evidence in judicial proceedings before courts of law in Nigeria.[21]

[18] The 1999 Constitution of the Federal Republic of Nigeria, section 1(1).
[19] Ibid.
[20] Ibid, ss 3.
[21] Evidence Act, 2011, Section 256.

To begin with, the Evidence Act provides that in any situation where a person has allegedly written or signed on a document, either wholly or partly, the person making such allegations must prove that the handwritten belongs to whom it is alleged to belong.[22]

Additionally, the Evidence Act postulates that in any circumstance whereby a rule of evidence has provided that a document must be signed, or has provided for certain consequences when a document is not signed, an electronic signature is enough to satisfy that provision.[23]

3.2.2 The Evidence Act 2023[24]

The Evidence Act was passed in 2023 to serve as an amendment Act amending the provisions of the 2011 Act in order to bring its provisions in accordance with global technological advancements in evidence taking which shall be applicable to all judicial proceedings in or before courts in Nigeria.[25]

While the Evidence Act 2011 has provided in section 93 that an electronic signature may be used in place of a traditional signature when the need for it arises, it failed to establish what an electronic signature connotes. This is one of the key amendments brought by the Evidence Act, 2023 which defines an electronic signature to mean authentication of any electronic

[22] Ibid. s 93(1).

[23] Ibid, ss2.

[24] Pertinent to bear in mind that that unlike how the passing of the Evidence Act 2011 was to repeal the Evidence Act 2004, the passing of the Evidence Act 2023 was not to repeal the 2011 Evidence Act, but to bring amendment and additions to some of its provisions, identifying the 2011 Evidence Act as the primary and principal Act, while the 2023 Act is the Amendment Act.

[25] The Evidence Act, 2023 Explanatory Memorandum.

record by a subscriber by means of electronic technique.[26] Additionally, the Amendment Act defines a digital signature as an electronically generated signature which is attached to an electronically transmitted document to verify its contents and the sender's identity.[27]

Flowing from the established, the Amendment Act made further amendment by inserting new sections of 84A - 84D. These new additions are a huge step forward in relation to electronic means of storing and transmitting information efficiently and conveniently.

Section 84A provides that if any law has provided for an information to be in written, typed or printed form, then such requirements will be fulfilled if the information is created in an electronic form.[28]

Similarly, the Amendment Act permits a person to authenticate an electronic record by affixing his digital signature on such records,[29] provided that the digital signature is considered reliable.[30] The reliability of such digital signature will then be established if its creation data or authentication data are linked to only the signatory, or only the authenticator;[31] the system is one such that if any changes or alterations are made to the signature or information,[32] it is easily detectable.[33]

---

[26] Evidence Act, 2011 (as amended in 2023), section 258.
[27] Ibid.
[28] Ibid, section 84A (a).
[29] The Evidence Act, 2011 (as amended in 2023) section 84C (1).
[30] Ibid, section 84C (2)(a).
[31] Ibid, ss. (3)(a).
[32] Ibid, ss. (3)(b).
[33] Ibid, ss. (3)(c).

Furthermore, it is provided that to the exclusion of secure digital signature, if any person has been alleged to have affixed his digital signature, it must be proven that the digital signature belongs to such person. When referring to a digital signature being secure, it means that only the signatory had the exclusive control as at the time of affixing such signature.[34]

A further addition made by the Amendment Act is the addition of the words "or digital signature" to "electronic signature" in the Principal Act.[35]

3.3 Cybercrimes (Prohibition, Prevention, etc.) Act 2015

Passed in 2015, the Cybercrimes Act operates as the principal and main enactment for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. In the context of electronic signature, the Cybercrimes Act stands as one of the notable enactments, hence the shed of the spotlight on the Act in this discourse.

According to the Cybercrimes Act, when purchasing a good or making any transactions, if a person makes use of an electronic signature in respect of the transaction, it shall be binding on the parties.[36] In view of this, if a person challenges the genuineness of such an electronic signature,

[34] Ibid, 84D.

[35] Prior to the addition, only an electronic signature maybe used to satisfy a document which is to be signed. With this addition, a digital signature or an electronic signature may be used in the place of a traditional handwritten signature.

[36] Cybercrimes Act, section 17 (a).

the person has the burden to prove that the signature does not belong to the signatory.[37]

As it is a well settled fact that the mere provision and criminalisation of an act without its punishment is a mere provision without a legal life, the Cybercrimes Act provides that in any such situation where a person intends to defraud or misrepresent by forging another person's electronic signature, such a person will be guilty of an offence, and be liable to conviction to imprisonment for a term of not more than 7 years or a fine of nothing more than ₦10,000,000 or both fine and imprisonment.[38]

Notably, the Cybercrimes Act has provided limitations to the use of electronic signature in respect of transactions involving certain documents, invalidating any such transaction if executed with an electronic signature. These documents include – creation and execution of wills, codicils and or other testamentary documents; Death certificate; Birth certificate; matters of family law such as marriage, divorce, adoption and other related issues; issuance of court orders, notices, official court documents such as affidavit, pleadings, motions and other related judicial documents and instruments; any cancellation or termination of utility services; any instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; any document ordering withdrawal of drugs, chemicals and any other material either on the ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.[39]

---

[37] Ibid, ss (b).
[38] Ibid, ss (c).
[39] Cybercrimes Act, Section 17(2)

3.4 National Information Technology Development Agency (NITDA) Act 2007

Yet another legal framework, the Act is responsible for the establishment of the National Information Technology Development agency to plan, develop and promote the use of information technology in Nigeria. Further the Act empowers NITDA to regulate IT practices and issue guidelines for e-commerce.

4.0 LEGAL VALIDITY AND ENFORCEABILITY OF ELECTRONIC SIGNATURES AND ELECTRONIC CONTRACTS

4.1 Requirements for validity of electronic signatures

Prior to 2023 when the Evidence Act (Amendment) Act, 2023 was passed, the principal Act[40] merely provides that an electronic signature suffices where a traditional signature would be required,[41] it does not provide for the requirements to be satisfied before it is held as valid. Given the amendment in 2023 however, section 258 of the principal Act was amended to address what an electronic signature is, as well as what digital signature connotes. Additionally, the new sections of 84A - 84D which were incorporated provide for electronic signature and the validity of same.[42]

---

[40] The Evidence Act, 2011, as amended in 2023.

[41] The Evidence Act, 2011, Section 93 (2).

[42] By virtue of Section 3 of the Evidence Act (Amendment) Act, 2023, the sections of 84A-84D were inserted into the Evidence Act, 2011.

According to the Act, an electronic or digital signature has to be one considered reliable.[43] Further, such a signature must be one to be proved.[44] In relation to the reliability of an electronic or digital signature, the creation data or authentication data of the signature are exclusively linked to the signature.[45] This implies that the key, password or device that is made use of in creating the signature must be linked uniquely and exclusively to the person signing.[46] Additionally, after the signature has been affixed, in any case the signature or information is altered, it must be detectable.[47]

In the context of proof, an electronic or digital signature must be proved to be within the exclusive control of the signatory at the time of affixing it; and it must be stored and affixed in such an exclusive manner as may be prescribed by the Act.[48]

4.2 Recognition of electronic contracts under Nigerian law

The digitalisation era has greatly influenced how things are carried on, and the way businesses are conducted. Contingent upon this, certain things which are traditionally carried on have shifted to making use of the internet. Businesses no longer have to meet to enter into agreements, the

[43] Evidence Act (Amendment) Act, 2023, s84C (2)(a)
[44] Ibid.
[45] Evidence Act, 2011 (as amended in 2023), s84C (3)
[46] The signature must not be one created by a shared password or generic account. If any other person has an access to the key used to sign, then it will not count as a reliable one, ie a thumbprint or FaceID used to approve a transaction will be reliable because it uniquely belongs to a person. While a shared office password used to sign a document will not be held as reliable because the access to it belies many users. Hence, "it is not linked to the signatory and no other person."
[47] Ibid, s 84C (2).
[48] Ibid, s84D.

formation of contract and conduct of transactions can easily be done without the requirement of a physical presence or interaction between parties.[49]

Although legal frameworks in relation to electronic contracts remain fragmented in Nigeria, it is not frowned against. The closest provisions in relations to electronic contracts include section 84 of the Evidence Act which provides that statements contained in electronic forms are admissible in court;[50] CAMA, 2020 supports the digital legal framework by recognising that if it is required that a company signs a document, it may be signed by a director, secretary or any other authorized officer of the company. And importantly, an electronic signature is legally valid and enforceable.[51]

4.3 Enforceability of Click-Wrap, Browse-Wrap, and Shrink-Wrap Agreements

In spite of the innovative solutions accompanying electronic contract, one controversy that has always been and continues to be in the spotlight remains as regards the validity of electronic contracts. [52] This is particularly due to the lack of a dedicated framework regulating these

[49] Marcus Okoko, 'Revisiting Electronic Contracts And Signatures: Perspectives On Digitisation And The Law In Nigeria' (*Mondaq,* 2022) available at https://www.mondaq.com/nigeria/contracts-and-commercial-law/1175714/revisiting-electronic-contracts-and-signatures-perspectives-on-digitisation-and-the-law-in-nigeria accessed 24 January, 2026.

[50] The Evidence Act, 2011 (as amended in 2023), Section 84.

[51] Companies and Allied Matters Act, 2020 section 101.

[52] Otebolaku, Oyindamola Ifeoluwa, 'Digital Signatures and Their Legal Implications Under the Evidence Amendment Act 2023' (*SSRN,* 2025) available at http://dx.doi.org/10.2139/ssrn.5345413 accessed 24 January, 2026.

contracts in Nigeria,[53] and the nature which these electronic contracts take, creating element of doubts in relations to the presence of the elements a contractual agreements when these agreements are entered into.

Despite the prevalence of these agreement questions arise as to their validity, and *inter alia*, their enforceability.[54] For a click-wrap agreement, instead of parties having to sign on a paper containing the terms of a contract, a mere "accept" suffices and creates a legally binding agreement between the parties. The question is thus, to what extent are these terms binding? As held in several court cases, for a click-wrap to be held binding, the consent of the user is actively required;[55] the terms which they are agreeing to must be prominently displayed;[56] when the terms are displayed, such terms should be easily understood by an average lay person properly informing such person of the nature of agreement he is entering into.[57]

For shrink-wrap agreements, these are more of frequent controversies than click-wrap agreements. This is due to the fact that this type of agreement deals with implied consent, and the terms of use are deemed

---

[53] Marcus Okoko, 'Revisiting Electronic Contracts And Signatures: Perspectives On Digitisation And The Law In Nigeria' (*Mondaq,* 2022) available at https://www.mondaq.com/nigeria/contracts-and-commercial-law/1175714/revisiting-electronic-contracts-and-signatures-perspectives-on-digitisation-and-the-law-in-nigeria accessed 24 January, 2026.

[54] Adam Gatt, 'Electronic Commerce — Click-Wrap Agreements: The Enforceability of Click-Wrap Agreements' (2002) 18(6) *Computer Law and Security Report* p. 404 – 410.

[55] *Feldman v. Google* 513 F. Supp. 2d 229 [E.D. Pa 2007]

[56] *Meyer v Uber Technologies, Inc*., 868 F.3d 66 (2d Cir. 2017).

[57] *Specht v Netscape Communications Corp.*, 150 F. Supp. 2d 585 (S.D.N.Y. 2001).

accepted by a person even before he views them. This however does not emasculate the validity of a shrink-wrap agreement, owing to the fact that a purchaser, after purchasing a product has the opportunity to review the terms and the shrink-wrap agreement, and return the product if he does not accept the terms.[58] Notably, the enforcement of this agreement lies not in the individual's purchase of the software, but the purchaser keeping the product till the expiration a stipulated return time.[59]

Before a browse-wrap agreement is held legally enforceable, the courts do not usually enforce it without having to inspect the nature of the agreement, and the manner in which the terms are displayed on the website. These agreements often require a greater level of scrutiny in determining its enforceability.[60]

4.4 Exceptions and Limitations: Documents Excluded from Electronic Execution

The passing of the Evidence (Amendment) Act, 2023 indicates an approval nod for electronic signatures in Nigeria. Consequently, it identifies that electronic signature can serve as a means in the place of a traditional signature. Nevertheless, this execution of documents is not limitless. There are certain documents, due to their nature, sensitivity, and other discerning features, that cannot be executed electronically. This provides to the effect that if these documents are executed through an electronic signature, they will not be valid.

---

[58] *ProCD, Inc. ProCD, Inc., v. Zeidenberg,* 86 F.3d 1447 (7th Cir. 1996)

[59] In *Brower v Gateway 2000, Inc.*, 676 N.Y.S.2d 569 (1st Dep't 1998), a purchaser who kept a computer beyond 30 days was held to have consented to the terms of an agreement.

[60] *Daniel Berman v Freedom Financial Network Llc*, No. 20-16900 (9th Cir. 2022)

According to the Cybercrimes Act, these documents include: creation and execution of wills, codicils and or other testamentary documents; Death certificate; Birth certificate; matters of family law such as marriage, divorce, adoption and other related issues; issuance of court orders, notices, official court documents such as affidavit, pleadings, motions and other related judicial documents and instruments; any cancellation or termination of utility services; any instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; any document ordering withdrawal of drugs, chemicals and any other material either on the ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.[61]

4.5 Electronic Signature and Electronic Contract under UNCITRAL

UNCITRAL[62] provides the legal framework for electronic transactions mainly through the Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures (2001).[63] These instruments are

[61] Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, section 17.

[62] The United Nations Commission on International Trade Law is a body of the United Nations established in 1966 to promote the harmonisation of international trade law. The primary aim of this body is to reduce legal barriers in cross-national transactions. The body does this by developing uniform legal rules that states can adopt in their regulations.

[63] The Model Law on Electronic Commerce (MLEC) aims to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce. In particular, it is intended to overcome obstacles arising from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for

largely based on the principles of functional equivalence and technology neutrality, ensuring that electronic signatures are not denied legal validity merely because they are in electronic form.[64] An electronic signature is regarded as valid where it is reliable for identifying the signatory and for indicating the signatory's approval of the information contained in the electronic record.

Similarly, UNCITRAL recognizes the validity of electronic contracts, provided the essential elements of a valid and enforceable contract, including offer, acceptance, intentions to create legal relations, and consents, are present. The Model Law affirms that contracts may be formed electronically and that communications such as emails or click-wrap agreements can constitute valid contractual exchanges. Flowing from this, it is placed that electronic contracts enjoy the same legal recognition and enforceability as traditional paper-based contracts under the UNCITRAL framework.

5.0 EVIDENTIAL CHALLENGES IN ELECTRONIC CONTRACTING

5.1 Authenticating the Signatory: Attribution and Identity Theft Risks

According to the Evidence Act, one of the requirements to a valid electronic signature is authentication. While this is aimed at ensuring

---

enabling the use of paperless communication, thus fostering efficiency in international trade.

[64] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce accessed 24 January, 2026.

security, it is not devoid of loopholes. Traditional signature has had a long-standing existence and acceptability to the extent that it has fostered trust, and is easily attributable due to its certain features. With recourse to this, it is appropriate to hold that an electronic signature cannot perform all the functions of a traditional signature.[65] When a signature is handwritten and signed on a paper, it enables forensic experts to scrutinise and detect any alterations or forgery by looking into the ink markings and handwriting of the signatories. It was argued that an electronic signature does not permit such detection as the content of an electronic signature may be altered, forged without detections or any trails being left behind.[66]

Moreover, anonymity is an inherent feature of the internet. While a mere click is enough to satisfy the acceptance of an offer in electronic contracting, it is practically impossible to prove the person behind the click. For an electronic signature to be held reliable, it has to be unique to the person signing it. This becomes an issue when such a person denies being one who signed, claiming that his account was accessed by a third party, a hacker or a family member to whom he has not delegated an authority to represent him.

In *Williams Group Australia Pty Ltd v Crocker,*[67] where the New South Wales Court of Appeal in Australia was to determine the validity of an electronic signature highlighted the heavy burden on a person to prove

[65] Dr. Anugbum Onuoha, Justice James Agbadufishim, Dr. Zuhair Jibril, 'Electronic Signature: Reviewing the Legal Issues on Its Validity and Authentication Under Nigeria Law' (2020) 8(5) *Global Journal of Politics and Law Research* 31.
[66] Ibid.
[67] [2016] NSWCA 265

that a document which bears his electronic signature was not affixed by him in such an occasion.[68]

5.2 Ensuring Data Integrity: System Reliability and Risk of Alteration

In traditional contract and signature, immutability is monumental, and when the records are fixed on a document, any changes made to such document in its terms are noticeable. It is no gainsaying the fact that for one of these reasons is why electronic contracts are still subjected to questions on the basis of their integrity and reliability. While this serves as a benefit when it provides the chance for it to be reused, by quickly adapting a new record and compiling a new one on existing records, it exists as a sword in its vulnerabilities, notably when the changes are not observable.[69]

---

[68] In that case, Mr Crocker was one of the three directors of IDH Modular Pty Ltd, a company established to supply building modules. The company makes use of an electronic signature system known as "HelloFax". With Mr Crocker's electronic signature, a credit application and personal guarantee were submitted to Williamss Group Australia Pty Ltd. Mr Crocker had been provided with a username and password by one of his co-directors to enable him to access the HelloFax system. He did not change the password during the relevant period, with the result that anyone who had these logins details would be able to affix Mr Crocker's electronic signature to documents. The central dispute was whether Mr Crocker was bound by the electronic signature despite not applying it by himself. Williams Group held that Mr Crocker had intended that whoever has the access to the account had the authority of Mr Crocker to bind him. The argument was rejected by the Court, while ruling that merely having an account and failing to secure it did not amount to representation of authority by Mr Crocker to affix his signature.

[69] Filip Boulderez, 'Digital Signatures and Electronic Records' (2005) *Antwerp.*

When referring to the integrity of electronic contract, the contention is not premised on the exact duplicate of terms as they were agreed or received, rather it is based on the functions, finality and purposes the terms are to serve.[70] This is better elucidated in a situation where the agreement between two parties having being finalised to mean a certain thing, and the other party, to his advantage, modifies the terms of the agreement at the detriment of the other person. In a traditional contract, when the written terms are modified, through indications like correction fluid, erasures, different ink, it easily attracts attention. Although in advanced electronic contracts and signatures, changes are easily noticed when advanced tools such as audit trails, timestamps, hashing are put in place, in simple contracts such as shrink-wrap agreements, typed names, unchecked documents it becomes hard to notice, and imposes heavy burden on a person to prove that the terms he agreed to have been modified.[71]

5.3 Problems of forgery, impersonation, and cyber fraud

Attributable to the conception of the internet, forgery, impersonation and cyber fraud are rampant in the order of the day. In order to gain unauthorised access to financial information, personal information, health records, critical information, cybercriminals make use of several methods in forging documents and impersonating victims.[72] Premised on this is why electronic contracts are heavily susceptible to cyber fraud.

---

[70] Ibid.

[71] Cybercrimes Act, s 17.

[72] Saleh, Ibtisam Mousa, and Abdul Raheem Adel Ghnaimat, 'Electronic Impersonation Crimes in the Jordanian Criminal Legislation: A Critical Analysis' (2025) *International Annals of Criminology* (2025) 280 available at https://doi.org/10.1017/cri.2025.10074 accessed 30 January, 2026.

Just as it is widely known, anonymity is one of the notable features of the internet. This feature justifies why personal and identity information is usually concealed, serving as an underserved shield and cover for persons of mischief intents.[73] Unlike a traditional signature which is more often than not affixed physically where the parties are able to assess each other's legitimacy and identity to make such agreement a legally binding agreement, the electronic counterparts are more vulnerable to unauthorised use by malicious users.[74] Against this backdrop, digital signature was designed to serve as a solution to the issue of identity. However, this does not totally devoid digital signature of fraud, not because of the weakness in the technology, but in human, technical and systemic vulnerabilities surrounding it.[75]

5.4 Burden of Proof and the Presumption of Regularity

According to the Cybercrimes Act, any person who contends that an electronic signature is invalid in respect of any transactions will have the burden on him to prove such claims.[76] While the Act has imposed such burden on the contender, it fails to take notice of the fact that an electronic signature is executed on a pseudonymous internet, stripping the burden of stability. In the traditional form, if a person contends the invalidity of a

---

[73] Hannah Olusoga-Tinubi, 'Legal Analysis of Electronic Signatures in Nigeria' (2018) 11(2) *African Journal of Stability & Development* 338 available at https://doi.org/10.53982/ajsd.2018.1102.08-j accessed 30 January, 2026.

[74] Ibid.

[75] Digital signature functions on private keys. Through phishing, malware or key-loggings, cybercriminals can access these keys and sign documents with the credentials. When this is done, the signed document reflects as signed in the name of the victim. This imposes yet another burden on the victim to prove that the document has not been signed by him.

[76] Cybercrimes Act, section 17(2).

signature, a handwriting expert may be called upon to assess it. However, when taken into the context of an electronic signature, a handwriting expert cannot possibly prove the validity of a click, forcing the law to rely on the reliability of the system used.

It is well settled in law that he who asserts must prove his assertion.[77] In an electronic contract, a person claiming the validity of an electronic contract must prove his assertion through a certificate of compliance in line with the provision of section 84 of the Evidence Act. Such an electronic document must first be tendered, after which it must be admitted. In the event of it not be admitted, such case fails.[78]

Moreover, the law presumes regularity in official acts. If an electronic contract is executed with a secure electronic system, the presumption of the law is that such signature had been fixed by the person to whom it correlates. The person now has the burden to prove otherwise when he claims otherwise by supporting his claims through technical evidence,[79] placing a heavy burden of credential negligence on the signatory.

5.5 Conditions for Admissibility: The Section 84 Compliance Certificate

[77] The Evidence Act, section 131.

[78] In *Kubor v Dickson* 2013 4 NWLR (PART 1345) 534 the trite principle of compliance with S. 84 of the Evidence Act, 2011 before tendering computer-generated evidence was established. Hence, tendering from the Bar, a computer printout of the online version of the Punch Newspaper, and another printout from the website of the Independent National Electoral Commission without evidence in relation to the use of the computer called to establish the above conditions made the document inadmissible.

[79] Io Moonwalkers Inc v Banc of America Merchant Services LLC (2018).

Under the Nigerian legal system, for electronic evidence to be presented and admitted by the court in evidence, it must strictly be in line with the provision of section 84 of the Evidence Act. The proponent must demonstrate compliance with specific statutory requirements, which are proven through a certificate.

In order to get document admitted, the party must prove that the document was produced by the computer during a period when the computer was used regularly to store or process information for the purpose of regular activities; during that period, information of the kind contained in the document was regularly supplied to the computer in the ordinary course of those activities; throughout the material part of that period, the computer was operating properly. If it was not operating properly or was out of operation for some time, that failure must not have affected the production of the document or the accuracy of its contents; the information in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.[80] Additionally, the Evidence Act provides that if an oral evidence cannot be provided, a certificate is enough to prove the proper operation of the computer.[81]

6.0 CONCLUSION

[80] The Evidence Act, 2011 section 84(2).

[81] Ibid, s 84(4); the certificate is identified as a certificate of compliance, and it must Identify the document containing the statement and describe the manner in which it was produced. Also, it must state the identification information of any device that was used in the production of that document in order to show that the document was produced by a computer, and it must be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities.

Conclusively, this work has identified what electronic contract is, as well as what electronic signature connotes. Additionally, it identified the relevant legal provisions regulating electronic contract and signatures in Nigeria, flowing from the Constitution to the provisions of the Evidence Act as amended in 2023. Further, it assesses the requirements for their validity, additionally providing for how their authentication and reliability can be proved. In the same vein, it has recognised the evidential challenges accompanying electronic transactions in Nigeria.

6.1 Judicial Capacity Building

There is a need for continuous training of judges and legal practitioners in line to advance in digital forensics. The bench must be equipped to distinguish between genuine system errors and frivolous it wasn't me defenses without relying solely on rigid technical certificates.

Additionally, section 84 of the Evidence Act should be reviewed. The strict requirement for a certificate of compliance should be liberalised for standard commercial transactions where no genuine dispute as to authenticity exists, mirroring the presumption of integrity found in the UNCITRAL Model Law.

Adoption of Digital ID Integration. Integrating electronic signatures with the National Identity Number (NIN) or Bank Verification Number (BVN) infrastructure would create a robust, non-repudiable identity layer, reduces fraud and making attribution easier to prove in court.