Legal Regime of Electronic Banking in Nigeria and The Evidence Act 2011: An Examination of The Intersection Between Technology and Law

DR. MAJEBI SAMUEL AMUNE
College of Law, Joseph Ayo Babalola University, Ilesa, Osun State, Nigeria

Abstract- ***The article examines the origin of electronic banking from a historical perspective and analyses the principles of the law of evidence applicable to electronic banking disputes and litigations in Nigeria. The article relies on primary and secondary sources of information. The primary source includes the Constitution of the Federal Republic of Nigeria 1999 (as altered), the Evidence Act 2011, the Evidence (Amendment) Act 2023, the Central Bank of Nigeria (CBN) Act 2007, Cyber Crimes (Prohibition, Prevention, Etc.) Act 2015, National Information Technology Development Agency (NITDA) Act, 2007, Nigerian Communications Act 2003, Economic and Financial Crimes Commission (Establishment, Etc.) Act, 2004 and Case Laws. The secondary source includes books, journal articles, and the Internet. This article reveals that the emergence of electronic banking has transformed the financial environment, providing unmatched convenience, rapidity, and accessibility. It further shows that the paradigm change has also brought about new challenges in the areas of e-banking disputes and litigations. It also reveals that the Evidence Act has not adequately addressed electronic records' vulnerabilities in banking disputes, litigations, and other challenges associated with modern technological usage. Furthermore, the article reveals that although the Evidence Act has made progress in dealing with the admissibility of electronic evidence, numerous unresolved issues still need to be addressed.***

Indexed Terms- ***Electronic Banking, Evidence Act 2011, Electronic Evidence, Admissibility, Nigeria***

I. INTRODUCTION

In the modern era, technology has become widespread, and its effect has been unavoidable. One of the industries that have undergone a remarkable transformation as a result of this revolution is the banking industry. The use of information and communication technologies (ICT) in providing banking services and goods has been a notable development in the industry. This has led to the emergence of electronic banking, also known as electronic funds transfers (EFTs). ICT-based products such as Automated Teller Machines (ATMs), pay-by-phone systems, and personal computer banking are some of the examples of electronic banking.

Electronic Funds Transfers (EFTs) are considered the third generation of payment systems, taking over from cash (notes and coins) and paper-based payment methods (like cheques). Electronic banking comes with several benefits for financial institutions and customers alike. It can enhance transaction processing speed, decrease costs, attract and retain customers, and offer greater convenience compared to traditional banking methods. By using electronic banking systems, customers can save time, money, and effort.

In the 1980s, the banking industry witnessed a significant development with the introduction of the Automated Clearing House (ACH) system in the United States. This system allowed banks to perform electronic transactions, which was a major milestone in the history of electronic banking. The ACH system paved the way for the development of modern electronic banking systems that we see today. With the advancements in Internet technology, electronic banking has become even more popular in the 21st century. Today, there are many innovative electronic banking systems available that offer a wide range of features and services. Mobile banking apps, for instance, allow customers to perform transactions and manage their finances using their smartphones. Online banking portals provide customers with access to their

accounts and allow them to perform various transactions using a web browser. Biometric authentication technologies, on the other hand, use fingerprint or facial recognition to enhance security and ensure that only authorised individuals can access their accounts.

These electronic banking systems have revolutionised the way people manage their finances and made banking more convenient than ever before. Customers can now perform transactions from the comfort of their homes or on-the-go using their smartphones. Moreover, these systems have made banking safer by incorporating advanced security measures that protect customer information from cyber threats and fraud.

The influence of technology and its advancements on our world today cannot be denied. Events around the globe are largely shaped by the radical development of technology. The digital revolution has profoundly altered how we create and store documents. According to a study, the majority of documents produced in many organisations today are in digital format, with a significant percentage never being printed[1]. As technology has become an integral component of our world and country, it is only natural to expect that laws should evolve to keep pace with technological dynamics. One way in which Nigerian laws have adapted to the changing landscape of technology is by allowing evidence generated from electronic sources to be admissible. The Evidence Act of 2011 permits documents created from electronic sources such as computers to be admissible, and also outlines the necessary conditions for electronic evidence to be admissible[2]. This statutory approval of the admissibility of electronic evidence is praiseworthy. It is especially noteworthy, as the rapid global growth in technology has resulted in increasingly complex problems that were not previously envisioned by statute. Therefore, the decision to allow the admissibility of electronic evidence demonstrates statutory awareness and responsiveness to the boundless innovativeness of technology.

Banks have consistently been at the forefront of leveraging advanced technology to enhance their products and services. This is primarily driven by the need to cater to a diverse customer base and the complex nature of their operations. The utilisation of electronic and telecommunication networks has enabled banks to offer a wide array of value-added products and services. Despite regulatory advancements in the sector, the Nigerian banking industry is unfortunately characterised by consumer exploitation. This exploitation encompasses imposing unrealistic and undisclosed charges, making unjustifiable deductions, levying Automated Teller Machine (ATM) fees without dispensing cash to customers, and maintaining slow complaint handling and redress mechanisms which may eventually lead to litigation against the bank by customers. Where this occurs, how do the courts handle such cases?

The Evidence Act of 2011 lacks a specific definition for electronic evidence. This may be because lawmakers aimed to avoid a definition that would quickly become outdated due to the rapid pace of technological advancements. Alternatively, electronic evidence is sometimes referred to as digital evidence, computer evidence, or computer-generated evidence. It's worth noting that the Nigerian judiciary permits the admissibility of electronic evidence in many landmark cases, but certain conditions must be met. For example, the authenticity, originality, and reliability of the electronic evidence must be established, and it must not have been tampered with or altered in any way.

Furthermore, it is important to consider the approach of courts in other jurisdictions regarding the admissibility of evidence generated from electronic sources such as computers. Understanding the judicial attitude towards the admissibility of electronic evidence in other jurisdictions is essential in assessing the level of compliance of Nigerian courts. It may also be useful in shaping the Nigerian legal system to ensure that the law keeps pace with the changing technological landscape.

There have been noteworthy advancements concerning the convergence of the law of evidence and the realm of electronic banking. Nigerian courts have increasingly recognised the validity of electronic evidence, provided it adheres to specified verification criteria. This acceptance represents a significant shift, facilitating more efficient and streamlined legal processes in the context of digital banking. Moreover, the legal framework now acknowledges electronic

signatures as binding and valid. This development empowers parties to enter into secure agreements without the necessity for traditional handwritten signatures, thereby enhancing efficiency in business transactions and legal commitments in the digital landscape. In terms of data protection, financial institutions in Nigeria are mandated to maintain the confidentiality and security of customer information. To fulfil this responsibility, they are required to implement robust cybersecurity measures that safeguard sensitive data against breaches or unauthorised access. This is crucial given the increasing incidences of cyber threats in the financial sector. Additionally, banks and other financial entities must maintain comprehensive electronic records as part of their operational practices. These records are essential not only for facilitating internal audits but also for ensuring compliance with regulatory frameworks. By doing so, financial institutions are better positioned to provide the necessary documentation during regulatory inspections or legal inquiries, thereby upholding transparency and accountability in their operations. Though there was no specific law just for electronic banking, several existing laws manage it indirectly. These include the Central Bank of Nigeria (CBN) Act, the Banking and Other Financial Institutions Act, and the Electronic Transactions (Prohibition) Act. These laws help protect customers' rights and ensure that electronic transactions are secure.[5]

However, notwithstanding the notable advancements in the field, several challenges that require additional reforms to ensure full alignment with international best practices persist. One significant issue is the authentication of electronic records, which remains a critical concern. Ensuring that digital documents can be reliably verified as genuine is essential for maintaining their credibility in legal and regulatory contexts. Additionally, the vulnerability of electronic evidence to alteration poses serious risks. Without robust safeguards in place, such evidence could be manipulated or tampered with, undermining its integrity and reliability in investigations and court proceedings.

Addressing these gaps would significantly enhance the effectiveness, reliability, and security of electronic banking in Nigeria, as well as improve the admissibility of electronic evidence in the country's legal system, especially in electronic banking disputes and litigations.

II. THE HISTORY OF EVIDENCE IN NIGERIA

The introduction of information technology has led us into an era of advanced digital communication. We can now transfer information quickly, conduct cross-border transactions, and complete electronic transactions. Automation has radically changed the landscape of human activities. These digital advancements have also transformed the way legal proceedings are conducted in courts worldwide.[6] Therefore, the law must keep up with modern developments. The use of computers and other electronic storage and communication systems has increased significantly in commercial and financial transactions, especially in the banking industry in Nigeria. The use of digital evidence has also increased in recent decades. Courts have allowed the use of electronic mail, digital photographs, logs of ATM transactions, word processing documents, instant message histories, spreadsheets saved from accounting programs, internet browser histories, databases, contents of computer memory, computer backups, computer printouts, tracks from Global Positioning Systems, logs from electronic door locks, and digital audio or video files. Electronic evidence has become crucial in resolving disputes or cases, whether criminal or civil. Nigerian law allows for the admissibility of electronic and computer-generated evidence through section 84 of the Evidence Act, 2011. The 2011 Evidence Act marks a turning point in the history of Nigeria's legal system. It not only allows for the admissibility of electronic and computer-generated evidence but also classifies it as documentary evidence. Therefore, just like other documentary evidence, electronic and computer-generated evidence can be proven by primary or secondary evidence. This paper focuses on the admissibility of electronic evidence in legal proceedings in Nigeria. It briefly discusses the concept of electronic evidence, sources of electronic evidence, proof of conditions for admissibility of computer-generated evidence, admissibility of electronic evidence in legal proceedings in Nigeria, challenges in

determining the probative value of electronic evidence, and international best practices.

On the other hand, technology has become an integral part of our lives in the 21st century, and the banking industry is no exception. Banks have adopted information and communication technologies (ICT) to provide services to their customers.[7] Electronic banking is one such example of ICT-based products that include Automated Teller Machines (ATMs), pay-by-phone systems, and personal computer banking. Electronic funds transfers (EFTs) are a part of electronic banking and are known as the third great age of payment, following payment by cash and paper-based payment such as cheques. EFTs are beneficial for both financial institutions and customers as they enable faster transactions, reduce costs, and offer convenience. Electronic banking first emerged in the 1980s, gained traction in the 20th century, and further flourished in the 21st century with the advent of the Internet. This trend has shifted towards the Internet as a medium for performing transactions electronically for both banks and customers. There has been a remarkable development of innovative electronic banking systems that have been commercially tested and developed since then.

Over the last ten years, the use of computers in Nigeria has skyrocketed. People rely on computers for financial transactions, communication systems, and even modern automobiles. We are now in an age where electronic devices are used for everyday transactions. When there are disputes, electronic evidence is often used to help resolve them.[8]

Electronic evidence has become increasingly popular in recent years as a way to prove facts in criminal investigations and civil cases. It is widely agreed that electronic evidence is crucial to help courts establish the truth in a case. When wrongdoers deny their guilt, all relevant evidence must be used to prove it, whether in civil cases, where the balance of probability is used, or in criminal cases, where the evidence must be beyond reasonable doubt. Proving cases is important because sometimes allegations turn out to be true even when there are consistent denials. Evidence can be based on oral or eyewitness testimony, but, when necessary, facts are available electronically, they must be presented.

The Nigerian Evidence Act of 2011 introduced a new concept in evidence law by making provision for the admissibility of evidence obtained by electronic means. Before this, the previous Evidence Act[9] did not allow for the use of computer-generated evidence. Although the Supreme Court of Nigeria had previously ruled in the case of Esso W.A. v Oyegbola[10] that computer print-outs were admissible as documentary evidence, there was no clear legal framework for the admissibility of this type of evidence.

The 2011 Act clarified the issue of admissibility of computer-generated evidence in section 84, which was further supported by the case of Kubor v Dickson.[11] This new provision was a welcome development as it helped to define the conditions for the use of electronic evidence in legal proceedings, especially banking-related cases.

We will examine how computer-generated evidence can be proven, as well as the admissibility of electronic evidence in legal proceedings in Nigeria. We will also discuss the challenges involved in determining the value of electronic evidence.

In the early 20th century, Nigeria's judicial system was characterised by the co-existence of two distinct legal systems. In the South, customary law, which was mainly unwritten, governed legal proceedings, while in the North, the practice, procedure, and evidence were based on the written rules of the Quran.[12] These legal frameworks have since evolved and are currently enforced by the various Customary and Sharia Courts throughout the country.[13] Furthermore, the application of English Law of Evidence was widespread across Nigeria due to Ordinance No. 4 of 1876, which facilitated the adoption of English Common Law, Equity, and Statutes of General Application enacted on or before January 1st, 1900,[14] until 1945.

The initial Evidence Ordinance[15] was passed in Nigeria in 1943 but was not implemented until 1945. This law was strongly influenced by Sir James Fitzgerald Stephen's Digest on Law of Evidence,[16] which aimed to organise the English Law of Evidence. Even after Nigeria gained independence in 1960, the Ordinance remained in force and was subsequently recognised as an Act.

Before the 1979 Constitution of Nigeria, the 1963 Constitution listed evidence under the concurrent Legislative List, giving the Regional Houses of Assembly the authority over evidence matters. However, in 1979, the 1979 Constitution of Nigeria transferred evidence from the Concurrent Legislative List to the Exclusive Legislative List.[17] As a result, the responsibility for matters related to evidence in court shifted from the Regional Houses of Assembly to the National Assembly.[18]

The Ordinance remained in effect until 2011 when it was revoked by the Evidence Act 2011. Prior to its revocation, the Act was included in the 1990[19] and 2004 Laws of the Federation of Nigeria (LFN), and its adoption into the LFN 2004 resulted in its current designation as Evidence Act,[20] or simply Evidence Act, 2004. The Act underwent an amendment in 1991 and remained largely unchanged until its repeal in 2011, marking the end of its 66-year existence.[21]

The failure to make additional revisions resulted in the Act becoming outdated in its handling of documents produced by computers. Despite other legislatures such as those in England and India updating their laws to encompass electronic documents in line with contemporary needs, the Nigerian legislature did not take any action regarding the Evidence Act. This inaction meant that documents and evidence generated by computers were not recognised under the Act. The Court of Appeal was among the first to publicly criticise the shortcomings of the Evidence Act in this regard. In Egbue v Araka[22], Pats-Acholonu, J.C.A (as he then was) observed that:

> It must be clearly understood that our Evidence Act is now more than 50 years old and is completely out of touch and out of tune with the realities of the present scientific and technological achievements. Most of its sections are archaic and anachronistic and need thorough overhaul to meet with the needs of our times. But alas it is with us now like an albatross on our neck...

The Nigerian Law Reform Commission (NLRC) referenced a statement from the New Zealand Law Commission in its 1998 Report, which provides an accurate description of Nigeria's current situation. The statement sheds light on the complexities and challenges faced by Nigeria thus:

> A serious criticism of our evidence law is that it hinders rather than search for the truth through the creation of artificial and unnecessary constraints on evidence which may be admitted. Instead of enhancing and facilitating the rational common-sense abilities of the judge and jury, the law makes it difficult to formulate a complete picture of what really happened. The focus is on the technicalities of the rules and their exceptions rather than the broader policies lying behind them.

Senator Akinyede introduced a bill to amend the Evidence Act 2004, recognising the need for updated legislation on evidence in Nigeria. The subsequent Evidence Act 2011, which took effect on 3rd June 2011, allowed for the admission of computer-generated evidence in legal proceedings, addressing limitations of the previous act and broadening the scope of what constituted documents. However, the Act presented challenges by failing to define certain terms related to electronic records and by not allowing for self-authentication of electronic evidence in court, leading to an amendment in 2023. This update included specific definitions for key terms like electronic records, electronic signatures, and digital signatures, and introduced safer methods of authenticating electronic evidence, electronic oath-taking, electronic gazette, and more. Despite these advancements, some challenges persist, which will be further discussed in this study.

2.1 Definition of Evidence by Various Writers

The process of defining any legal concept often leads to a wide array of thoughts and opinions. These perspectives are derived from various sources, including authoritative judicial figures and relevant statutes. These sources offer potential solutions to the challenge of defining legal concepts. Evidence can be broadly described as anything that sheds light on, proves, or aids in establishing the truth of factual matters within a given context. This encompasses a range of elements, such as testimony, written documentation, physical objects, and other forms of evidence presented in a court setting to demonstrate the existence of a fact. Additionally, evidence is any

form of tangible or verbal material that can be utilised to bolster the existence of a factual assertion.[23]

The term "evidence" refers to information that helps prove facts. The law of evidence consists of rules governing how facts can be proven in courts, tribunals, and arbitrations. It is a set of rules that determine what evidence can be presented in legal proceedings. These rules are considered adjectival, meaning they describe how evidence should be used, rather than being substantive laws themselves.

The W.B. Best defined evidence as any matter of fact, the effect, tendency, or design of which is to produce in the mind a persuasion affirmative or disaffirmation of the existence of some other matter of fact.[24]

According to Black's Law Dictionary,[25]

> Evidence is defined as "something (including testimony, documents, and tangible objects) that tends to prove or disprove the existence of an alleged fact…the collective mass of things presented before a tribunal in a given dispute.

It is important to note that from the above definitions, "fact" is a key element in the matter of evidence, as every trial aims to ascertain and establish the fact. These definitions are not the same as the usage of the word in a court of law. The law of Evidence is very important in court. Courts use evidence to decide which facts can be considered and how to establish those facts.[26] When someone goes to court, the court needs to look into the case, draw conclusions from the facts, and listen to legal arguments to find the truth and achieve justice.[27] There is no one definition of evidence, and different people have different ideas about what it means.

According to Phipson, evidence means "the testimony whether oral, documentary or real, which may be legally received to prove or disprove some facts in dispute".[28]

Cross defines evidence as "the testimony, hearsay, documents, things and facts which a court will accept as evidence of facts in issue in a given case."[29] However, Dr. K.O. Amusa points out a flaw in this definition. According to Dr. Amusa, the definition is limited to only those things that the court of law will accept or act upon. This overlooks the fact that evidence includes both admissible and inadmissible evidence. For example, if a document is deemed inadmissible, it will not be returned to the person who presented it. Instead, it will be marked as rejected and retained by the court as part of the record proceedings. Additionally, the definition fails to acknowledge that evidence comprises facts used to prove or disprove the facts in question.[30]

Furthermore, Cross and Tapper said that:

> the evidence of the fact is that which tends to prove it – something which may satisfy an inquirer of the fact's existence. Courts of law usually have to find that certain facts exist before pronouncing on the rights, duties and liabilities of the parties, and such evidence as they will receive in furtherance of this task is described as judicial evidence.[31]

On his part, Osadolor defines evidence in terms of its purpose when he posited as follows:

> … evidence is the means by which an alleged matter or fact is established or disproved…. Evidence is the mandatory weapon in the arsenal of litigants employed in convincing a trial judge and ultimately assisting the trial judge in arriving at justice.[32]

Nokes defined judicial evidence as "evidence received by court of justice in proof or disproof of facts, the existence of which becomes a question before them".[33]

Aguda sums up the concept of evidence as it is relevant to our present discourse as follows:

> a court, faced with the problem of the determination of a suit before it can solve such a problem only after making an inquiry into the facts of the case, drawing inferences from those facts, and listening to argument of parties to the case or of their counsel. Evidence is the means by which facts are proved, but excluding inferences and argument. It is common knowledge that a fact can be prove by oral testimony of persons who perceived the fact, or by the production of documents, or by the inspection of things or places – all these will come within the meaning of judicial evidence. On a very broad view, it is sometime

> permissible to include in this list such other means of proving a fact as admission and confession, judicial notice, presumption and estoppels… Sometimes the word 'evidence' is used in connection with admissibility, for example, when it is said that something is not evidence, it may mean that, that thing is not admissible evidence.[34]

Fidelis Nwadialo, a Nigerian jurist and legal scholar, defines evidence as "any matter of fact, the effect, existence, or non-existence of which is to be judicially investigated or decided, and which is capable of being proved at a judicial trial or inquiry."[35] This definition encompasses the core idea that evidence is any fact or circumstance presented in a legal proceeding to support or refute a claim and can be proven or disproven through various means, such as testimony, documents, or physical objects.

Furthermore, Fidelis Nwadialo[36] chose not to cover computer-generated evidence in his work, citing the absence of specific Nigerian laws on the subject for inclusion in a book on Nigerian law of Evidence. He argued that any pronouncement on it would be more suitable for journals rather than formal textbooks on the law of Evidence. However, he acknowledged that any evidence admissible under common law before the passing of the Act would still be admissible,[37] as per the then section 5(a) of the Evidence Act and decisions of the West African Court of Appeal (WACA)[38] and the Federal Supreme Court.[39]

In his article "Admissibility of Electronically Generated Evidence," Amupitan J.[40] emphasised the importance of giving liberal interpretation to the admissibility of electronic evidence in Nigerian courts and worldwide. He stressed that this is crucial in the modern age of information technology to ensure that the law remains relevant and effective, thus enhancing judicial activism.

Yemi Osinbajo[41] has expressed his belief that computer printouts should not be considered original documents. He has also disagreed with certain English court decisions that consider computer-generated evidence to be "real evidence," even if it is based on statutory provisions. The author argues[42] that these computer printouts do not meet the criteria for documentary evidence as outlined in section 91 (formerly section 90) of the Evidence Act. In conclusion, he suggests that without amending the Evidence Act, Nigerian courts will find it challenging to accept computer-and electronically generated evidence.

In my personal view, the esteemed author was correct, and I firmly support the idea that this led to the inclusion of Section 83 in the 2011 Evidence Act. However, while these authors have shared their perspectives on electronically generated evidence, their discussions lack an in-depth exploration of the topic.

The above definitions have invariably discussed merely what evidence is all about without identifying the challenges of its application to e-banking disputes and litigations which is the purpose of this study. The focus is to bridge the gaps in the above definitions which occurred as a result of the writers not mentioning or discussing the challenges likely to result from the application of the principles of the law of evidence to e-banking disputes and litigations.

2.2 Classification of Evidence in Judicial Proceedings
The Law of Evidence applies to all areas of law and comes from various sources, including local laws and custom, the English Common Law, doctrines of Equity, statutes of general application in force in England as of January 1, 1900, local legislations and judicial interpretation based on them, Law Reports, Text Books, and Monographs on Nigerian Law, and Judicial Precedents.[43] The main source of the Law of Evidence in Nigeria is the Evidence Act 2011, which contains the essential provisions relating to evidence. However, if necessary, any relevant statute such as the Constitution may be referred to for additional guidance.

Section 3 of the Evidence Act 2011 states that nothing in the Act will impact the admissibility of any evidence that is made admissible by any other legislation validly in force in Nigeria. However, the Evidence Act 2011 does not address the admissibility of a piece of evidence that is admissible at common law, unlike the Evidence Act Cap E 14 Laws of the Federation 2004, which allows the admission of evidence under the rules of the English Common Law.

The Common Law of England is a source of the Nigerian Law of Evidence when the Evidence Act 2011 is silent on a matter or when there is a gap in the Nigerian Law of Evidence. This is consistent with the position in Onyewusi v Okpukpara,[44] where the court stated that it is the Evidence Act or, if the Act is silent, the Common Law of England that applies in the High Court.

However, the rules of the Common Law of England on Evidence cannot exclude any evidence that is admissible under the Evidence Act 2011 or any other statute applicable in Nigeria. Similarly, any evidence declared inadmissible by the Evidence Act 2011 cannot be admitted by any rule of English Common Law on Evidence.

If the provisions of the Evidence Act 2011 conflict with the provisions of the Constitution of the Federal Republic of Nigeria, the provisions of the Evidence Act 2011 will be declared null and void to the extent of the inconsistency. However, if the provisions of the Evidence Act 2011 conflict with the English Common Law rules on evidence or any other statute, the Evidence Act 2011 will prevail.

The Evidence Act 2011 categorises judicial evidence into oral evidence, real evidence, documentary evidence, and circumstantial evidence.

2.2.1 Oral Evidence:

The viva voce testimony, or oral evidence, refers to a person's spoken assertion offered as proof of the truth of what is being asserted. This type of evidence is typically provided by a witness under oath or affirmation in a court's witness box. Oral evidence, often known as testimonial evidence, is considered the most credible means of establishing a case in court. It is the most common type of judicial evidence and holds several advantages. One advantage is that it allows the court to observe the demeanour and behaviour of the witness, helping to determine their credibility. Additionally, oral evidence enables the opposing party to cross-examine the witness or witnesses.[45] It is important to note that oral evidence must be provided by a witness who claims to have seen, perceived, or heard the relevant facts.

2.2.2 Real Evidence:

Real evidence, in the legal context, refers to tangible objects presented for examination in court. This type of evidence encompasses physical items other than documents that are submitted for the court's review. It serves as an objective and demonstrative means of proof, derived from the inspection of actual objects such as locations, individuals, animals, or items. A notable example is the case of Lyon v Taylor,[46] in which the court mandated the presentation of a dangerous and troublesome dog for assessment. Notably, real evidence can be transported to the court for examination, or if impractical, inspection can be conducted at the location where the object is situated.[47]

2.2.3 Documentary Evidence

The term "documentary evidence" refers to a statement in a document that is presented to the court to prove a fact in question. This type of evidence can be divided into two categories:

i. Primary Evidence: This category includes the original document itself,[48] also known as the Best Evidence Rule. This rule originates from the old English common law and emphasises the requirement for the best evidence to be presented. According to Lord Hardwicke in the case of Omichund v Barker,[49] “the judges and sages of the Law have laid it down that there is but one general rule of evidence, the best that the nature of the case allows.”

Section 258 of the Evidence Act defines a document. If multiple duplicates or copies of the same document are created through the same process (e.g., typing with carbon paper), each copy, including the original, is considered primary evidence of the document, as established in the case of Esso W.A Incorporated v Oladiji.[50]

ii. Secondary Evidence: This category encompasses a copy of the original document.[51] Secondary evidence may include certified copies provided under specific provisions, copies made from the original using mechanical processes that ensure accuracy, copies compared with the original, copies made from or compared with such copies, counterparts of documents against parties who did not execute them, and oral accounts of the

document's contents given by an individual who has seen it. For further insight, refer to the case of Aina v Jinadu.[52]

2.2.4 Circumstantial Evidence

Several circumstances which when accepted make a complete and unbroken chain of evidence. By this, it means evidence not of the fact in the issue but of other facts from which the fact in the issue can be inferred. In most cases, it is difficult to get direct evidence thus recourse may be heard as circumstantial evidence to establish a case in court. It is to be noted however that before an accused can be convicted on circumstantial evidence such evidence must be irresistibly and mathematically point to one direction namely that the accused committed the offence for which he is standing trial. It is usually contrasted with direct evidence. In Adeniyi v The State,[53] the accused was the last person seen with the deceased alive. He was in the deceased car a day after they were both seen together. He led the police to a place where the skull and bones of the deceased were recovered together with the lost material she wore and a necklace with the pendant insignia "R" which stands for Regina, the name of the deceased. In that circumstance, he was convicted for the murder of the said Regina. See also Chioma Ejiofor v The State.[54]

2.2.5 Direct Evidence

This is a testimony that pertains to facts directly perceived by a witness through one of their senses. It serves as evidence for a fact that is currently being disputed. This type of evidence is presented by a witness to support the truth of the asserted fact. Direct evidence encompasses real evidence. In cases where direct testimony from an eyewitness is unavailable, the court is authorised to draw inferences from established facts to demonstrate the existence of other logically inferable facts. Direct evidence is evidence that, if accepted as true, establishes a fact in question without the need for the court to rely on inference or presumption.

2.2.6 Original and Hearsay Evidence

Generally, statements, written or oral, made by persons who are not called as witnesses are not admissible in evidence. Still, they are relevant and admissible in the circumstances mentioned in sections 39 to 55 of the Act. When evidence of such a statement is offered only as proof that the statement was made, irrespective of whether they are true or false, such evidence is called Original Evidence. But when a third party repeats the statements as proof of the contents of the statement, this will be regarded as hearsay evidence and therefore generally inadmissible.[55]

2.3 Conceptual Clarifications

2.3.1 Evidence

Evidence is anything that can help to prove or disprove a fact in a legal case. This can include testimony, documents, or tangible objects.[56] Although there is no clear definition of evidence in the Civil Evidence Act, the PACE Act, or the Nigerian Evidence Act 2011, the Supreme Court of Nigeria has defined evidence to include the "means by which any alleged matter of fact, the truth of which is submitted to investigation, is established or approved".[57] This can include oral or documentary testimony or physical objects. Evidence is used to inform courts of the issues of facts as ascertained by the pleadings. In summary, evidence is any legally admissible information that may help to prove or disprove a fact in dispute.

The law of evidence plays a crucial role in the legal system, as it determines the admissibility of evidence in trials. It dictates what can be presented to prove or disprove a fact in an issue and outlines the manner in which evidence can be admitted by the court. This includes but is not limited to witness testimony, documents, physical objects, and expert opinions. The law of evidence ensures that the evidence presented is reliable, relevant, and fair, ultimately contributing to the pursuit of justice in legal proceedings.[58]

The Indian Evidence Act of 1872 outlines what constitutes evidence, providing a comprehensive framework for understanding its various categories. According to section 3 of the Indian Evidence Act 1872,59 "evidence" encompasses:

i. All statements permitted or required by the court from witnesses;
ii. Statements or declarations made by the parties involved or their agents; and
iii. The contents of documents, which include electronic records presented to prove a fact.

In simpler terms, evidence under the Indian Evidence Act 1872 can be categorised into three primary forms namely:

i. Oral Statements which refer to the verbal accounts or testimonies of witnesses during court proceedings;
ii. Statements by Parties or Agents which include both written and verbal statements made by the parties involved in a case or their representatives; and
iii. Documentary Evidence which comprises the contents of documents, which also extends to electronic records.

Understanding the definition and categories of evidence outlined in the Indian Evidence Act is crucial for legal practitioners and parties involved in litigation. It lays the groundwork for how evidence is admitted and assessed by the courts, thereby influencing the outcome of legal proceedings. It provides a clear and structured definition of evidence, which is vital for the administration of justice. By classifying evidence into testimonial, documentary, and real evidence, it ensures a comprehensive approach to evaluating information presented in court. This framework not only aids in understanding legal proceedings but also highlights the importance of evidence in establishing facts and reaching fair judgments in the judicial system.

In the same vein, the Nigerian Evidence Act 2011 recognises three forms of evidence namely: oral, documentary and real.[60] The term "evidence" when used in a legal setting tends to have various interpretations,[61] for instance, it may mean the legal process by which the court is formally made aware of the essential points or claims presented in the pleadings submitted by the parties involved in a case. Evidence can be said to be that which is brought before the court to prove or disprove a fact in issue, either orally, documentarily, or by way of real evidence. Sometimes, even if relevant, evidence can be required by law or the court to be supported with other evidence before it can be admitted in court.[62] An example of such evidence is electronic evidence which requires a method of authentication and oral evidence from the maker of such document before it can be admitted.

2.3.2 Electronic Evidence

The term 'electronic evidence' refers to the digital information that can be used as evidence in court. This includes data created, stored or transmitted via any electronic device, computer or communication system.

Electronic evidence, often referred to as digital evidence, encompasses any type of information that is stored or transmitted in binary form[63] and may be relied upon in court.[64] This can include emails, text messages, social media posts, digital images, videos, databases, and any other digital files. The probative value of electronic evidence refers to its relevance and reliability in establishing facts in a legal proceeding. It includes evidence generated from a wide range of sources, such as computers, cameras, the internet, the dark web, closed-circuit television (CCTV), and more. In the description, it comprises three (3) elements namely, all forms of data (including digital files, emails, and documents), devices for storing information (such as hard drives, servers, and cloud storage), and "information that has potential to make factual account of either party more probable or less probable that it would be without evidence" (which encompasses anything that can be used to support or refute a claim, including witness testimony, physical objects, and expert analysis).[65]

Meanwhile, the Evidence Act 2011 does not define electronic evidence,[66] but the definition by Schafer and Mason is commonly used.[67] This definition focuses on data that has the potential to make the factual account of either party more probable or less probable than it would be without evidence. It has three elements: first, any data created, manipulated or stored in a computer; second, any devices used to store or transmit data; and third, the concept of evidence as information that can affect the factual account of a case.[68] It is important to note that electronic evidence is not limited to data generated or stored on computers and can include many different types of electronic devices. Thus, electronic evidence is any raw fact stored in an electronic device. It can be presented in court to prove or disprove a relevant fact.

Nevertheless, electronic evidence has distinct characteristics that set it apart from other forms of evidence and these unique aspects consist of, but are not restricted to, an electronic signature.

Electronic Signature is also known as a digital signature and is defined as any data in electronic form that is attached to or logically associated with other electronic data and is used to demonstrate the authentication and integrity of the document. Electronic signatures use cryptographic techniques to ensure that the signature is uniquely linked to the signatory and the data being signed.[69] This provides an added layer of security and trust, making electronic signatures a reliable and widely accepted method for validating the authenticity of electronic documents. Electronic signature is a highly efficient and time-saving method for obtaining signatures on electronic documents. This method is legally recognised and supported by various laws and regulations across different countries and regions worldwide,[70] making it a secure and reliable way to conduct business transactions and formalise agreements.

In the United States, an electronic signature is legally defined as a computer data compilation of any symbol or series of symbols, created and executed by an individual to bind the signer to the contents of a document. This electronic signature is considered to be the legal equivalent of the individual's handwritten signature[71] and is recognised as such under the Electronic Signatures in Global and National Commerce Act (ESIGN) and the Uniform Electronic Transactions Act (UETA).

The concept of electronic signature, as defined in Section 2 of the United Nations Commission on International Law (UNCITRAL) Model Law, refers to data in electronic form that is affixed to or logically associated with a data message. This electronic signature may be used to identify the signatory to the data message and indicate the signatory's approval of the information contained in the data message. On the other hand, a digital signature is a specific type of electronic signature that involves a numerical method of providing authenticity to digital records and documents. It offers the recipient assurance that the document is from a known sender and has not been altered in transit.[72]

In Nigeria, the concept of electronic signature and digital signature was not legally defined until the Evidence Act was amended in 2023. The Amendment Act specifically defines an electronic signature as the authentication of any electronic record by a subscriber using the electronic technique specified by law, which includes a digital signature. This legal definition provides clarity and sets the foundation for the use of electronic and digital signatures in various transactions and communications within Nigeria's legal framework.[73]

A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital message, document, or software. It is created using a mathematical algorithm that generates a unique digital fingerprint for the content being signed. This fingerprint is then encrypted using the signer's private key, and the encrypted signature is attached to the digital content. When the signature is verified using the signer's public key, it provides assurance that the content has not been altered and that it was indeed signed by the expected sender. Digital signatures are often used in electronic transactions, contracts, and official communications to ensure the security and authenticity of the involved parties.

Furthermore, the amendment to the Evidence Act 2011 provides legal recognition and validity to electronic signatures, including digital signatures, ensuring their enforceability and admissibility in electronic records and transactions. For the avoidance of doubt, the amendment provides that:

> Where a rule of evidence requires a signature or provides for certain consequences if a document is not signed; an electronic signature or digital signature satisfies that rule of law and avoids those consequences.[74]

The implication of the above is that the legality of an electronic or digital signature is considered equivalent to that of a handwritten signature, thus providing assurance of the document's authenticity and ownership. Electronic signatures use cryptographic techniques to validate the identity of the signer and ensure the integrity of the signed document. On the other hand, digital signatures are based on a specific type of electronic signature that involves a certificate-based digital ID to verify the signer's identity and ensure that the document has not been altered since it was signed. This technological advancement not only adds to the integrity of data but also significantly

reduces the risk of fraud and security issues.[75] In simple terms, both electronic and digital signatures serve to authenticate the author and link them to the contents of the document. This can be achieved through various methods such as attaching names, watermarks, or even using biometric data for verification.[76]

An electronic record is an information stored in a computer system or an electronic machine.[77] It includes data, images, or sounds stored, received, or sent in an electronic form or microfilm.[78] This content can be created, modified, archived, maintained, retrieved, or distributed using computer systems or electronic devices.[79] Digital media encompasses a wide range of formats, including documents, images, videos, music, presentations, and more. It has become an integral part of modern communication, entertainment, and information sharing.

Using electronic evidence has become more popular in recent years for proving facts in criminal investigations and civil cases. It is widely agreed that electronic evidence plays an important role in helping courts find the truth. When someone is accused of wrongdoing, they often deny it. To prove guilt, all relevant evidence must be presented, including electronic evidence. This is important for both civil cases, where the evidence must prove something is more likely than not, and criminal cases, where the evidence must prove guilt beyond a reasonable doubt. Proving cases is important because sometimes allegations turn out to be true despite strong denials. Evidence can come from witnesses or testimony. However, when the necessary facts cannot be proven this way, electronic evidence must be presented.

Stemming from the above, computer-generated evidence could be said to be any evidence that is generated from a computer or other digital devices such as electronic multimedia or telecommunications devices. This includes any evidence that can be found in digital photographs, e-mails, instant message histories, word processing documents, spreadsheets, internet browser histories, databases, computer memory contents, ATM transaction logs, computer backups, computer printouts, tracks from Global Positioning Systems, logs from electronic door locks in hotels, digital audio or video files, etc.

Therefore, electronic records refer to any type of information that is stored in an automated device, such as a computer, smartphone, or server. These records can include emails, documents, databases, or any other type of digital information. According to the law, electronic records can be presented as evidence in court without requiring the original physical copy, as long as they meet specific legal conditions for admissibility. This means that if an electronic record satisfies the legal requirements, it can be used as evidence without the need to produce the original document.

To understand the history of electronic evidence admissibility, we need to look at the development of evidence law in Nigeria. Nigeria's legal system, including evidence law, was influenced by England due to its colonial history. When colonial rule was established, courts were created to administer justice. However, there were no codified rules of evidence at that time. Instead, the courts applied the English Common Law of Evidence.[80]

In 1943, Nigeria introduced the Evidence Ordinance to codify the rules of evidence in a single document. This was the first attempt to do so in the country. The Evidence Act of 1945 was created based on Sir James Fitzgerald Stephen's Digest of the Law of Evidence and was an important milestone in the development of the law of Evidence in Nigeria. However, it only attempted to codify the existing English Common Law of Evidence.

The Evidence Act of 1945 remained unchanged and was the only source of evidence law in Nigeria until 2011 when it was finally amended. This was a significant issue because the Act remained unaltered for over 65 years, despite the technological advancements in Nigeria during that period. This is in contrast to Britain and other countries that amended their Evidence Law to allow for the admissibility of scientific and forensic evidence.[81]

The Evidence Act of 1945 did not keep up with modern technology in Nigeria. This meant that evidence generated electronically was not accepted in court. This caused many problems in the justice system. The legislature did not make enough changes to the act. But in 2011, the Evidence Act was updated.

It improved the law of evidence in Nigeria, especially regarding electronic evidence. Documents from computers can now be used as evidence, as long as certain conditions are met. This change has helped a lot in the Nigerian court system.

Specifically, it is provided that a statement present in a computer-generated document can be presented as evidence in any legal proceeding. However, this is only possible if certain conditions specified in subsection (2) of this section are met. The statement should pertain to a fact that could have been provided as direct oral evidence.[82]

It is further provided as follows:

i. That the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or by any individual;
ii. That over the period, there was regularly supplied to the computer in the ordinary course of those activities, information of the kind contained in the statement or of the kind from which the information so contained is derived;
iii. That throughout the material part of that period, the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during the part of that period was not such as to affect the production of the document or the accuracy of its contents; and
iv. That the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.[83]

Thus, in recent times, electronic evidence has become admissible in courts of law. However, this admission is subject to certain conditions, which must be fulfilled for electronic evidence to be considered valid and acceptable. These conditions include the authenticity of the electronic evidence, its relevance to the case at hand, and the accuracy of the evidence. The electronic evidence must also be obtained legally and be stored in a secure and tamper-proof manner until the time of its submission in court. Given these conditions are met, electronic evidence can be presented in court and used to support or refute a case.

2.3.3 Admissibility and Relevancy

Within the realm of legal evidence, the concept of admissibility holds significant weight as it pertains to the acceptability of presented evidence in a court of law.[84] For evidence to be deemed admissible, it must first meet the necessary criteria for presentation. Regardless of its relevance to the case at hand, all evidence must undergo a rigorous admissibility examination before its consideration in court.[85]

The rules for admitting evidence in civil and criminal proceedings are different. In civil cases, the Supreme Court, in Torti v Ukpabi & Ors.,[86] outlined the conditions for admissibility as follows:

i. Whether the evidence has been pleaded
ii. Whether it is relevant
iii. Whether its admissibility is not excluded by any rule of law

In criminal cases, the proof of evidence is similar to pleadings in civil trials.[87] In civil trials, facts that are not pleaded are inadmissible, while in criminal trials, facts not stated in the proof of evidence may be tendered and admitted. However, both parties are bound by their pleadings, and evidence of facts not pleaded are not admissible.

In the case of Amadi v. A-G Imo State,[88] the court held that the proof of evidence does not have to contain every bit of evidence that the prosecution requires as long as it contains relevant and sufficient facts to sustain a prima facie case against the accused person.

In criminal trials, admissibility of facts, whether stated in the proof of evidence or not, is governed by their relevance and other strict rules of admissibility relating to free and fair trial. In civil trials, the court may have discretion whether or not to reject inadmissible evidence, but in criminal trials, it is under a duty to reject such evidence.[89] Thus, it can be concluded that rules of admissibility are more stringent in criminal trials than in civil ones.

The terms relevancy and admissibility may seem to be closely related, but they actually have distinct meanings within the context of law. Relevancy pertains to the suitability of evidence as a basis for reasoning, while admissibility concerns whether evidence is permissible under the law.[90] It is worth noting that although these terms may appear to be closely intertwined, what is admissible must also be relevant. Admissibility, therefore, determines whether a piece of evidence can be presented in a trial,[91] and this determination is based on its relevancy. In legal proceedings, only evidence that is admissible under the law can be presented in court. Consequently, the rules governing the exclusion of evidence, as outlined in section 1 of the Evidence Act, will be applicable whenever the issue of admissibility arises in court.[92] Moreover, the Supreme Court has sought to simplify the criteria for admissibility by stating that a document shall only be admissible if it has been pleaded, is relevant to the fact in question, and is admissible under the law.[93]

The term "relevance" in the legal context refers to whether a piece of evidence is connected to the facts before the court and is more likely to be true than not based on human reasoning. In both civil and criminal proceedings, counsels must demonstrate that the evidence they are presenting is crucial to the case before it can be admitted by the court. This requirement ensures that only relevant evidence is considered during trial, preventing the introduction of unnecessary or prejudicial information. Additionally, relevance can be established by showing a clear connection between the facts being presented and the legal elements of the case.[94] This ensures that the evidence being considered is directly related to the issues at hand and is not based on speculation or conjecture.

The other side of the argument is that not all relevant evidence is admissible. For instance, if an electronically generated document is sought to be used in court as evidence without proper authentication or oral evidence of the maker in court, it may be considered relevant in the proceedings but may not be admissible by the court due to lack of proper verification. Additionally, if a court admits a document that is not relevant, it is then responsible for expunging or disregarding such wrongful admission. Failure to do so can result in complications within the legal process,[95] and the appellate court is also entitled by law to expunge such document.[96] The rules governing the wrongful admission and rejection of evidence, particularly in legal proceedings, are crucial for ensuring fair and just legal processes, as they dictate what evidence can be presented and considered in court. Adhering to these rules helps prevent the introduction of unreliable or prejudicial evidence, ultimately safeguarding the integrity of the judicial system.[97]

2.3.4 Computer

According to the Cambridge online dictionary, a computer is an electronic device that quickly calculates data. It is used for storing, writing, organising, and sharing information electronically, or for controlling other machines.[98] Similarly, section 5(6) of the Civil Evidence Act and section 258(1) of the Nigerian Evidence Act 2011 define a computer as any device for storing and processing information. Any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison, or any other process.

Based on the above definitions, we can conclude that any device used to store and process data can be considered a computer. Therefore, mainframes, desktop and laptop computers, tablets, and smartphones are some of the different examples of computers.[99]

2.3.5 Document

You can establish a fact in an issue by presenting a piece of documentary evidence such as contracts, emails, letters, or any other written or recorded material.[100] It is important to note that documentary evidence is challenging to explain.[101] The term usually refers to “a document providing information about something”.[102] The traditional definition of a document is often limited to anything written on paper. However, this narrow definition fails to capture the true essence of a document.[103] In reality, a document can be defined as anything written and presented as evidence in court.[104] For something to be considered a document, it must have two essential components: a written inscription and an object on which the inscription is made. Therefore, the material on which

the inscription is made should not be a determining factor in classifying something as a document.[105] In essence, a document does not have to be written on paper to hold the status of a document.

Before 2011 in Nigeria, the old Evidence Act limited the meaning of documents[106] and did not include electronically generated documents. Thus, the admissibility of electronically generated documents presented a challenge for both parties involved in legal proceedings and the judicial system. Section 2 of the Evidence Act 2004[107] defined document as:

Books, maps, plans, drawings, photographs and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than of these means, intended to be used or which may by means of letters, figures or marks or by more than one of these means, intended to be used or which may be for the purpose of recording that matter.

The court in Nuba Commercial Ltd v NAL Merchant Bank[108] ruled that computer-generated information was inadmissible according to the statutory definition. The case involved a party attempting to submit bank statements stored in a computer, but the court rejected them as inadmissible, stating that they did not fall within the definition of a document under the statute. Similarly, in the case of Elder Okon Aaron Udoro & Ors. v Governor of Akwa Ibom State & Ors.,[109] the Court of Appeal held that section 2 of the Evidence Act, 2004 did not encompass a video cassette, as it was considered a motion picture and not something inscribed on paper.

The definition of a document as outlined in the Act, along with the court's understanding of what constitutes a document, led to a general agreement among legal experts that the scope of the document definition was insufficient. This consensus among jurists, combined with ongoing advocacy from the judiciary, prompted calls for the legislature to expand the definition of a document. This continued until 2011 when a new Evidence Act was enacted.

The Evidence Act of 2011 provides a comprehensive definition of a document, encompassing a wide range of written, printed, or electronic materials that can be used as evidence in legal proceedings and it includes:

a. Books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter;

b. Any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it, and

c. Any film, negative, tape or other device in which one or more visual Images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it; and

d. Any device by means of which information is recorded. Stored or retrievable including computer output.[110]

The recent Act has broadened the definition of a document to encompass electronically generated documents as well as electronic devices. This means that courts can now accept an electronic device as evidence produced from a computer during legal proceedings. The Supreme Court has held that the use of "includes" in a statute expands its scope.[111] Consequently, the use of the word "includes" in the section extends the definition of a document to encompass even items not explicitly mentioned in the Act for future reference. As a result, it has been determined that plastic bottles bearing trademarks are considered documents.[112] In Nigeria, electronic documents are not classified under any specific type of evidence; instead, they are treated as constituting their own category of evidence.

The Nigerian Evidence Act 2011 has defined document to the effect that document includes books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance using letters, figures or marks or by more than one of these means, intended to be used or which may be used to record that matter; any disc, tape, sound track or other devices in which sounds or other data (not being visual images) are embodied to be capable (with or without the aid of some other

equipment) of being reproduced from it; and any film, negative, tape or other devices in which one or more visual images are embodied to be capable (with or without the aid of some other equipment) of being reproduced from it; and any device through which information is recorded, stored or retrievable including computer output.[113]

The definition starts with the word 'includes', which means the meaning of the document is broadened to items listed in the definition. The ejusdem generis rule of interpretation must be used so that anything similar to those listed in the definition will also qualify as a document in judicial proceedings. The definition of documents includes modern means of information storage and retrieval such as computer databases contained in hard drives, CD-ROMs, Magnetic Discs, Flash Disks, and Floppy Diskettes, as well as Motion Pictures recorded in Videotapes, Cassettes, Compact Discs, Micro Films, Micro Fiches, etc. Any information stored in a mobile phone will qualify as a document within the context of the definition. Similarly, by paragraph (d) above, a document may also be interpreted to include smartphones, laptop and desktop computers, digital cameras, etc. as they are devices capable of recording, storing or retrieving information.

2.3.6 Electronic Banking

Electronic banking is a broad term that refers to the process through which customers can conduct personal or commercial banking transactions and access information about financial products and services using electronic and telecommunication means over a public or private network. Electronic banking is essential because it provides cost-effective banking services. Through various electronic banking channels, funds can be swiftly moved domestically and internationally. In other words, electronic banking, which is also called web-based banking, e-banking, virtual banking, or online banking, is a way to use phones or computers to do personal finance tasks without going to a bank. It uses the internet and other electronic networks to give you access to financial services and products. You can do things like check your account balance and make transactions.[114]

Electronic banking is a way to do banking without the need for human interaction. It uses computers, phones, and other technologies to help you do things like transfer money, pay bills, deposit your paycheck, and buy things with your mobile phone. Banks have secure websites and mobile apps that let you see your account balance, transfer money, buy certificates of deposit (CDs), and buy and sell stocks and bonds if you have a brokerage account. Electronic banking has made it so that we don't need to move paper money and coins around as much as we used to. This means we no longer need people to help with every banking transaction.

E-banking comes in three basic types: Internet banking, Smart card banking, and Mobile/telephone banking. Internet banking allows customers to do their banking through the Internet. They can buy goods, pay invoices, and have products delivered to them, all from the comfort of their homes or offices. Smart card banking involves using electronic cards such as ATM, debit, or credit cards to access cash, make transfers, and check account balances without visiting a bank. These services are available at places like supermarkets, hotels, and shopping malls. Mobile/telephone banking lets customers conduct banking activities using mobile phones or fixed wireless phones. Customers

2.4 Legal Frameworks

2.4.1 Central Bank of Nigeria Act[115]

The lack of specific regulations is the primary obstacle to the widespread adoption of digital banking among Nigerian consumers. However, certain laws do play a crucial role in governing the country's electronic banking operations. One such law is the Central Bank of Nigeria Act.

The Central Bank of Nigeria has been established by an Act of the National Assembly to regulate banks and their services in Nigeria. The Act aims to promote stability and financial management in the country,[116] and it includes the Banks and Other Financial Institutions Act (BOFIA). The Central Bank of Nigeria has the power to promote a sound financial system in Nigeria.[117] To enhance security when accessing customers' personal information and data in the banking system, the Banker's Committee and all banks in Nigeria introduced the Bank Verification Number (BVN).[118] The governor of CBN released the regulatory framework for BVN to ensure the security

of the electronic payments system in Nigeria. Although there may not be any specific legislation on electronic banking yet in Nigeria, the CBN has proactively ensured compliance with best practices in the banking sector.

2.4.2 Cyber Crimes (Prohibition, Prevention, Etc.) Act, 2015

The Cyber Crime Act is a law passed by the National Assembly in Nigeria to ensure the protection of electronic communications, networks, data, and computer programs, and to promote cyber security. It serves as a regulatory and institutional framework for the country's prevention, prohibition, prosecution, and punishment of cyber crimes.[119] The Act imposes penalties for fraudulent activities carried out online, such as scams and other forms of internet-based fraud. Some examples of cyber-crimes that are punishable under this Act include intentionally accessing a computer system or network for fraudulent purposes, obtaining data that is vital to national security, securing access to any program, commercial or industrial secrets or classified information with the intent to commit fraud, and perpetrating any form of online or electronic fraud.[120]

Financial institutions that conduct electronic financial transactions are required by law to confirm their customers' identity. Customers are asked to provide documents with their name, address, and other relevant information for this confirmation. After the customer's identity has been confirmed, they may receive an ATM card, debit card, credit card, or any other electronic device.[121] The Cyber Crimes Act is an important law regulating internet use for electronic transactions in Nigeria. This Act covers all forms of electronic transactions, including online banking. Although the Act does not mention digital banking, it is still relevant in this context.

Service providers such as telecommunication companies also should ensure that customer data is protected in accordance with their right to privacy as provided for in the Constitution.[122] The Cyber Crimes Act also includes provisions that regulate the circumstances under which service providers may release consumer data or electronic communication or activities to law enforcement agencies.[123]

In other words, the Cybercrime Act acknowledges the use of electronic signatures for the purchase of goods and other transactions. This marks a significant departure from the Central Bank of Nigeria Guidelines on Electronic Banking, which previously prohibited reliance on digital signatures. The Cybercrime Act also penalises several acts, including fraudulent use of electronic signatures, passwords, or any unique personal identification feature. Additionally, the Act addresses fraudulent activities such as unauthorised electronic fund transfers and manipulation of ATM or Point of Sale terminals to commit fraud. These provisions offer legal recourse to victims of electronic fraud, enabling them to pursue criminal charges against cyber criminals. The Act also includes provisions for restitution to individuals who have suffered losses due to electronic fraud. Notably, the Act places responsibilities on financial institutions to implement effective counter-fraud measures and provide clear authorisation for debits or prompt reversal of unauthorised debits. However, some provisions, like Section 19(3), which requires customers to prove negligence on the part of financial institutions in case of a security breach, may pose challenges for customers. Nevertheless, the Cybercrime Act represents a positive step in addressing cyber-security issues, particularly in electronic banking.

2.4.3 National Information Technology Development Agency (NITDA) Act, 2007

The National Information Technology Development Agency (NITDA) Act of 2007 established the National Information Technology Development Agency in Nigeria. The agency is responsible for monitoring, evaluating, coordinating, and regulating Information Technology practices in Nigeria.[124] It also develops guidelines for electronic governance and monitors electronic data interchange in government, private sectors, and public sectors. The Nigerian Data Protection Regulations of 2019 protect people's privacy rights and control and safeguard data. These two laws regulate digital transactions in Nigeria, especially data protection. Although digital banking is not explicitly referred to in these laws, Section 6 of the NITDA Act shows that data protection in digital banking or transactions is regulated under this Act through the agency it established.

2.4.4 Banks and Other Financial Institutions Act (BOFIA)

The banking activities of financial institutions in Nigeria are regulated by the Banking and Other Financial Institutions Act (BOFIA).[125] While the act does not have any provisions for digital banking in Nigeria,[126] it grants regulatory powers to the Central Bank of Nigeria (CBN) to oversee the operations of banks and other financial institutions. The Governor of the CBN has the authority to make rules and regulations for the operation and control of all institutions under the supervision of the CBN, as per Section 58 of the act. It's worth noting that operating any form of banking in Nigeria without a license is prohibited under the act, and unlicensed financial institutions are not allowed.[127]

2.4.5 The Nigerian Communications Act, 2003

The Nigerian Communications Act is a set of rules for how telecommunications are used and operated in Nigeria.[128] Digital banking is only possible with the help of telecommunication platforms that enhance internet usage. In Nigeria, there are telecommunication companies such as Globacom Ltd., MTN, Airtel, and 9mobile, which provide a network for internet access. The Nigerian Communications Act established the Nigerian Communications Commission,[129] which is responsible for regulating the operation of these telecommunication companies in Nigeria and ensuring that they comply with the Act's provisions.

To operate in Nigeria, telecommunication companies must obtain a license from the Commission.[130] The license may be suspended or revoked by the Commission if the company violates the provisions of the Act, subsidiary regulations, or any other relevant written law in the telecommunications industry.[131] This provision means that telecommunication companies that regulate and protect the data privacy rights of individuals may have their licenses suspended or revoked if they violate those rights.

Although the Act does not explicitly regulate digital banking in Nigeria, it obligates telecommunication companies to work with other institutions, bodies, and agencies, banks inclusive, to protect the digital rights of individuals.

2.4.6 Economic and Financial Crimes Commission (Establishment, Etc.) Act, 2004.

The Economic and Financial Crimes Commission (Establishment, Etc.) Act is a law that applies to the entire country. The Act created the Economic and Financial Crimes Commission (EFCC)[132] as an agency responsible for enforcing the Act's provisions. One of the Act's powers is to investigate all financial crimes, including Advanced Fee Fraud and computer credit card fraud, and to take measures to trace, freeze, or seize the proceeds of such crimes.[133]

Section 6 of the Act allows the Commission to investigate any fraud related to digital banking. Additionally, the Act empowers the Commission to ask a bank or any other financial institution to provide information about a customer, produce books and documents related to such an account, and freeze the account. In other words, the Act gives the Chairman of the Commission or an authorised officer the power to instruct a bank or financial institution to provide account information and documents for the person under arrest. They can also require the bank to stop any transactions related to the account.[134]

However, the court has held that the Commission cannot unilaterally freeze or stop outward payments or operations of an account without a court order. That is, the court has held that banks must have a court order before freezing a customer's account or placing any form of restraint on any bank account.[135] According to Section 34 (1) of the Economic and Financial Crime Commission Act, 2004, the Economic and Financial Crime Commission has no power to instruct banks to freeze a customer’s account without a court order. Doing so would violate the customer's rights.

2.4.7 The Electronic Transactions Act 2011

The Electronic Transactions Act offers a thorough legal foundation for electronic commerce and online business activities in Nigeria. It recognises electronic transactions as legally enforceable, permits electronic signatures, and establishes robust authentication methods, ensuring the integrity of online interactions. Additionally, the law acknowledges electronic records as equivalent to traditional paper-based documents, facilitating digital storage and management.

The legislation also prioritises security, mandating measures to safeguard electronic transactions and data,[136] while protecting consumer rights through provisions like transaction cancellation and refunds.[137] Clear dispute resolution procedures are established, and the National Information

Technology Development Agency (NITDA) is empowered to regulate and oversee electronic transactions, ensuring best practices and standards are implemented for the benefit of all stakeholders.

2.4.8 Evidence Act 2011

This Act explains that the definition of "document" includes electronic records. This means that electronic data can be used as evidence.[138] It further discusses the admissibility of electronic records in legal proceedings. It allows electronic records to be presented as evidence[139] while section 86 outlines methods for authenticating electronic records and explains how the authenticity of electronic data can be established. Section 87 establishes requirements for proving the reliability and trustworthiness of electronic evidence and deals with the proof of electronic records. Section 258 defines "computer-generated document" and recognises the admissibility of documents generated by computers.

It is important to note that electronic records must be related to the important facts and only include necessary evidence in legal proceedings. It must be proven to be genuine to show that it is trustworthy and reliable. This sets standards for using electronic data in court.

The Act provides for a Certificate of Authenticity providing a formal method for verifying the authenticity of electronic records. An affidavit of authenticity offers an alternative means of establishing the credibility of electronic evidence through a sworn statement. Oral testimony of the maker allows the individual responsible for creating the electronic record to provide testimony regarding its authenticity.

Meanwhile, under the Evidence Act 2011, there is limited guidance on electronic evidence handling, indicating a need for further clarity and direction in managing electronic evidence in legal proceedings. No clear provisions for digital signatures, highlighting a gap in addressing the use of digital signatures as a method of authentication. No specific rules for audio-visual evidence, underscoring the absence of guidelines for the admissibility and handling of audio-visual electronic evidence.

2.4.9 Evidence (Amendment) Act 2023

On June 12, 2023, President Bola Ahmed Tinubu signed the Evidence (Amendment) Act 2023 into law. This new Act updates the Evidence Act 2011 by adding modern features like electronic oath-taking and electronic gazettes. It also broadens the use of computer-generated evidence and the verification of electronic records.[140] The Act now allows electronic records to be used as evidence in court, following global technological advances. An electronic record includes any data, images, or sounds that are stored, received, or sent electronically or on microfilm. The term "electronic record" has been added alongside "document" in the section about computer-generated evidence in the Principal Act. This means that both documents and electronic records can be accepted as evidence in court, as long as they meet the requirements outlined in the Act.[141] Electronic records that are printed on paper, stored, recorded, or copied in optical or magnetic media, or in a cloud database, are now usually considered documents. They can be accepted in Nigerian courts without needing to show the original, as long as the conditions in the Act are met.[142] The Act recognises that digital signatures can be used in court documents and legal processes. A digital signature is an electronic signature that is created and attached to a document that is sent electronically. This helps verify the document's contents, its authenticity, and the identity of the sender.[143] You can now confirm an electronic record by adding the maker's digital signature to it.[144]A digital signature is considered reliable only if: it links the signatory to the signature and no one else; any changes to the digital signature after it has been created can be detected; and any changes to the information after it has been signed can also be detected.[145] If someone claims that a digital signature was added to an electronic record, it must be proven that the signature belongs to the person who signed it.[146] To prove that a digital signature is genuine, you only need to show that when the signature was created, the signer's signature data was only in the signer’s control.[147]

The Act now allows for electronic oath-taking for affidavits and other documents that require an oath. People can submit affidavits electronically, which will save time in court and speed up proceedings. Additionally, the Act permits affidavits to be created using audio-visual methods, but only through authorised individuals who can take affidavits. A copy of the affidavit must be filed at the court's registry.[148]

The implications of these amendments are far-reaching. They include enhanced admissibility of electronic evidence, improved efficiency in trial administration, alignment with global technological advancements, and increased reliability and security of electronic records.

Furthermore, the amended Evidence Act brings Nigeria's legal framework closer to the UK's approach, particularly in recognising computer evidence as real evidence.

2.5 Theoretical Framework for E-Banking

The theoretical foundation for electronic banking encompasses various important models and theories that provide insights into the adoption and utilisation of e-banking services by individuals and organisations. Some of the notable theories include the Technology Acceptance Model (TAM),[149] the Diffusion of Innovations Theory,[150] and the Unified Theory of Acceptance and Use of Technology (UTAUT).[151] These theories help us understand the factors influencing the adoption and usage of electronic banking services.

2.5.1 Technology Acceptance Model (TAM)

i. Perceived Usefulness: This component emphasises the belief that utilising e-banking services can lead to enhanced job performance or personal convenience. Users who perceive substantial benefits from e-banking are more likely to embrace its use in their daily activities.
ii. Perceived Ease of Use: This refers to the belief that adopting e-banking will involve minimal effort. If users perceive the technology as user-friendly, they are more inclined to adopt it, reducing resistance to change.[152]

2.5.2 Unified Theory of Acceptance and Use of Technology (UTAUT)

i. Performance Expectancy: This construct gauges the degree to which individuals believe that the use of e-banking will provide them with significant gains in efficiency and productivity, influencing their willingness to engage with the technology.
ii. Effort Expectancy: Similar to TAM's perceived ease of use, this aspect measures how effortless the user believes the technology will be to use. A higher expectation of ease can correlate to increased adoption.
iii. Social Influence: This reflects the perceived impact of social networks on an individual's decision to use e-banking services. If individuals believe that peers or authority figures endorse e-banking, they are more likely to adopt it themselves.
iv. Facilitating Conditions: This factor encompasses the belief in the availability of organisational and technical support mechanisms necessary for successful e-banking use. Adequate infrastructure is essential for overcoming potential hurdles in the adoption process.[153]

2.5.3 Institutional Theory[154]

i. Regulatory Support: This component highlights the critical role that regulatory bodies play in endorsing and facilitating the adoption of e-banking services. A positive regulatory environment is essential for building consumer trust, as it establishes a framework that ensures the security and reliability of such services. Effective regulations can include guidelines for data protection, fraud prevention measures, and clear channels for consumer recourse in case of disputes. When consumers feel confident that there are robust protections in place, they are more likely to embrace e-banking as a legitimate and secure method for managing their finances. Consequently, a supportive regulatory landscape not only safeguards consumers but also fosters innovation and encourages financial institutions to expand their e-banking offerings.
ii. Institutional Influence: This aspect examines how prevailing institutional norms, values, and operating practices influence an organisation's

acceptance and integration of e-banking. Organisations often tailor their e-banking services to align with the dominant cultural and operational expectations within their industry or sector. For instance, a bank may design its digital services to reflect traditional banking principles, ensuring that they resonate with the established behaviours and expectations of its clientele. Additionally, the influence of institutional reputation, customer demographics, and competitive practices can further shape how an organisation adopts and promotes e-banking. By conforming to these institutional influences, organisations can enhance their credibility and acceptance among consumers, ultimately leading to a more successful implementation of e-banking solutions.[155]

2.5.4 Perceived Risk Theory

Perceived Risk: This concept highlights users' apprehensions about potential negative outcomes associated with e-banking, such as risks related to cybersecurity, privacy violations, and the potential for financial loss. Addressing these concerns is critical for fostering trust and enhancing adoption.

2.5.5 Perceived Benefits

i. Cost Savings: E-banking services often lead to reduced transaction costs, particularly for routine banking activities, making them more financially attractive to users.
ii. Convenience: One of the most significant advantages of e-banking is the ability to access banking services 24/7 from virtually any location, which appeals to a modern, mobile consumer base.
iii. Improved Service Quality: E-banking can enhance service delivery, offering faster transaction times and enabling more efficient customer service through digital platforms.[156]

2.5.6 Organisational Capabilities

i. ICT Readiness: Pertains to an organisation’s preparedness to adopt and implement the information and communication technologies necessary for e-banking.
ii. Financial Institutions Readiness: This reflects the willingness and capability of financial institutions to support the provision of e-banking services, from both technical and operational perspectives.

Together, these models and theories form a comprehensive framework that elucidates the multifaceted reasons influencing the adoption and usage of e-banking services. By leveraging this framework, researchers and practitioners can identify critical drivers and barriers to e-banking adoption, enabling the development of targeted strategies for effectively promoting and implementing e-banking solutions.

The theories mentioned indirectly integrate utilitarianism by prioritising functional advantages, increased efficiency, convenience, user-friendliness, and practical benefits.

Utilitarianism focuses on maximising overall well-being, happiness, or utility. In the realm of e-banking, these theories aid in understanding how users evaluate the advantages and disadvantages of embracing and utilising electronic banking services.

The utilitarian theory of e-banking underscores the practical benefits and overall usefulness that electronic banking services offer to customers.[157] Grounded in utilitarianism, this principle asserts that actions are morally right if they result in the greatest happiness or benefit for the largest number of individuals. Consequently, e-banking services are assessed based on their capacity to maximise positive outcomes for the greatest number of users. Here is a detailed breakdown of how this theory applies to e-banking:

1. Convenience and Accessibility: E-banking empowers users to conduct financial transactions at their convenience, anytime and anywhere, significantly enhancing accessibility. This eliminates the need for physical visits to banks, saving valuable time and effort.
2. Efficiency and Speed: E-banking transactions are typically faster than traditional banking methods, benefitting both users and banks by streamlining processes and reducing operational costs.
3. Cost-Effectiveness: E-banking can reduce transaction costs for users by eliminating fees associated with physical banking services. For banks, it minimises the need for physical

infrastructure and staffing, resulting in substantial cost savings.
4. Enhanced Security: Despite associated risks, e-banking often incorporates advanced security measures such as encryption and multi-factor authentication, enhancing the overall security of financial transactions compared to traditional methods.
5. Environmental Impact: E-banking contributes to environmental sustainability by reducing the need for paper-based transactions and physical travel to bank branches.
6. Financial Inclusion: E-banking can extend banking services to underserved populations, including those in remote or rural areas, thereby promoting financial inclusion and economic development.[158]

In the realm of E-Banking, the focus is on delivering functional benefits such as convenience, efficiency, and practical advantages that align with utilitarian principles. Users engage in a cost-benefit analysis, weighing the benefits of time-saving and accessibility against potential costs such as security risks and fees. E-Banking platforms prioritise user experience by emphasising ease of use, intuitive interfaces, and minimising cognitive load. This reflects the utilitarian concerns of users. Risk management is crucial, with E-Banking services working to mitigate risks such as security and privacy to ensure overall well-being.

Various theories encompassing utilitarianism come into play in E-Banking. For instance, the Technology Acceptance Model (TAM) considers perceived usefulness (PU) and perceived ease of use (PEU) as key reflections of utilitarian concerns. The Unified Theory of Acceptance and Use of Technology (UTAUT) aligns with utilitarianism through its focus on performance expectancy (PE) and effort expectancy (EE). Additionally, the Diffusion of Innovations Theory highlights how the relative advantage and complexity dimensions relate to utilitarianism.[159]

Utilitarian principles are integrated into E-Banking strategy by aiming to maximise convenience through streamlined processes and reduced cognitive load. Risk minimisation is achieved by implementing robust security measures and ensuring data protection. Furthermore, efforts are made to optimise user experience through user testing and gathering feedback, while also providing clear information regarding fees, terms, and conditions.

Examples of utilitarianism in E-Banking include mobile banking apps with intuitive interfaces, online bill payment systems with automated reminders, secure encryption methods for transactions, and personalised financial management tools.

REFERENCES

[1] Julian Gillespie, and others, “Coping When Everything is Digital? Digital Documents and Issues in Document Retention” (2004) Baker and McKenzie Cyberspace Law and Policy Centre White Paper, at p 4 http://www.cyberlawcentre.org/ddr/ddr_wp_A4.pdf accessed on 22nd November 2024.

[2] Section 84 of the Evidence Act, 2011.

[3] https://www.runlawjournals.com/index.php/runlawj/article/viewFile/76/60?form=MG0AV3 accessed 6th November 2024.

[4] https://oer.biu.edu.ng/wp-content/uploads/2020/02/ADMISSIBILITY_OF_ELECTRONIC_EVIDENCE_IN_NIGERIA_-_-1.pdf?form=MG0AV3 accessed 6th November 2024.

[5] https://thenigerialawyer.com/electronic-banking-and-the-rights-of-the-customer-in-nigeria/?form=MG0AV3 accessed 6th November 2024.

[6] Charles C.A, “An Examination of the Concept of Electronic Funds Transfer System in Electronic Banking and the Law” cited by Muhammed A. D. and Tijjani M. B. “Appraisal of the e Admissibility of Electronic Evidence in Nigeria and the Possibility of Its Application Under Sharia” https://www.academia.edu/37209893/Appraisal_of_the_Admissibilty_of_Electronic_of_Possibility_of_its_Application_Under_Sharia accessed 16th November 2024.

[7] https://www.cbn.gov.ng/OUT/CIRCULARS/BSD/2007/GUIDELINES%20ON%20ELECTRONIC%20BANKING%20IN%20NIGERIA.PDF?form=MG0AV3.

[8] S.J. Apochi, 'Admissibility of Electronically Generated Evidence Under The Nigerian Evidence Act, 2011: Challenges And Prospects', JETIR March 2021, Vol. 8, Issue 3 https://www.jetir.org/papers/JETIR2103337.pdf?form=MG0AV3 accessed 16th November 2024.

[9] Cap. E14 LFN 2004

[10] (1969) NMLR 194

[11] (2013) 4 NWLR (Pt. 1345) P. 534

[12] G. Arishe and D.O Oriakhogba, The Evidence Act, 2011: Closing the Window for the Application of Common Law Rules of Evidence. https://Www.Researchgate.Net/Publication/329681796_The_Evidence_Act_2011_Closing_The_Window_For_The_Application_Of_Common_Law_Rules_Of_Evidence <Accessed On 11th November, 2022 accessed 6th October 2024.

[13] T. A. Aguda, *Law and Practice Relating to Evidence in Nigeria*, (2nd ed. Lagos: MIJ Professional Publishers, 1998).

[14] F. Nwadialo, *Modern Nigerian Law of Evidence*, (2nd ed., Lagos: University of Lagos Press, 1999).

[15] No. 27 of 1943.

[16] The 1945 Ordinance appears to have been heavily influenced by both the English and Indian Evidence Acts, as evidenced by the similarities between them. This connection is further supported by the fact that the Indian Evidence Act of 1892 was instrumental in shaping the 1945 Ordinance.

[17] G. Arishe and D.O Oriakhogba, (n 4).

[18] C.E. Adah, The Nigerian Law of Evidence, (Malthouse Press 2000) 3.

[19] Cap. 112.

[20] Cap. E14 LFN 2004.

[21] See (n 9) supra.

[22] (1969) NMLR 19.

[23] Wigmore J.H., *Wigmore on Evidence,* (5th ed. USA: Aspen Publishers, 2012).

[24] Best W.M., *Principles of The Law of Evidence,* (14th ed. London: Sweet & Maxwell, 2018).

[25] Bryan A. Garner, *Black's Law Dictionary*, (8th ed. USA: West Publishing Co., 2004).

[26] *Evidence Act, 2011* Cap E. 14.

[27] Morgan E., *Introduction to The American Law Institute; Model Code of Evidence*, (Philadelphia: The American Law Institute,1942).

[28] Phipson R., *Phipson on Evidence*, (13th Edn, Sweet & Maxwell 1982).

[29] Cross R., *Cross on Evidence,* (9th ed. London: Butterworths, 2017).

[30] Dr. Amusa K. O., Department of Public Law, University of Lagos. *"Lecture Note on Definition of Evidence" given on the 2nd of August, 2004https://www.academia.edu/49239896/A_CRITICAL_APPRAISAL_OF_THE_RELEVANCE_AND_ADMISSIBILITY_OF_ELECTRONICALLY_GENERATED_EVIDENCE* accessed 4 September 2024.

[31] C. Tapper, *Cross and Tapper on Evidence*, (London: Butterworths, 1999).

[32] F. O. Osadolor, *Source Book on the Law and Practice of Evidence in Nigeria,* (Benin: Daveprint Associate, 2004).

[33] Nokes G., *An Introduction to Evidence*, (4th ed. London: Sweet & Maxwell, 1967).

[34] See (n5) supra.

[35] See (n6) supra.

[36] *Ibid.*

[37] *Ibid*.

[38] *Onyeanwusi v Okpukpara* (1953) 14 WACA 311.

[39] *R. v Itule* (1961) 1 All NLR 462.

[40] J. Amupitan Lecture Note on Law of Evidence. A University of Jos Lecturer.

[41] Yemi Osinbajo; *"Admissibility of Computer-Generated Evidence under Nigeria Law",* (1990) *jus*, vol .1 no 1. p.260

[42] Ibid at pages 253 – 255.

[43] Sanni O., 'The Complete Guide to Sources of Evidence Law', https://djetlawyer.com/sources-of-evidence/?form=MG0AV3 accessed 13th November 2024.

[44] (1953) 14 WACA

[45] Fidelis Nwadialo, (n6) Supra p. 10.

[46] (1862) 3F & F.731.

[47] Section 127 Evidence Act 2011.

[48] See Section 86 (1-4) Evidence Act 2011.

[49] (1744) Willes 534, 550.

[50] (1968) NMLR 453.

[51] Section 87 Evidence Act 2011.

[52] (1992) 4 NWLR (pt.233)91.

[53] (2001) FWLR pt. 57, pg. 809.

[54] (2001) FWLR pt. 49, pg. 1457.

[55] See *Subramanian v Public Prosecutor* (1956) I WLR 965.

[56] *Ibid*.

[57] *Tukur v UBA & Ors.* (2012) LPELR - 9337 (SC).

[58] Simon Cooper et al, Cases and Materials on Evidence, (4th Edn, Blackstone Press Limited 1997) 1.

[59] The Nigerian Evidence Act 2011 follows the model of the Evidence Act of 1872 as amended.

[60] Oral evidence is testimony given verbally in court, typically by a witness. Documentary evidence, as the name suggests, encompasses all documents and electronic records presented in court for examination (as per section 3 of the Indian Evidence Act, 1872, as amended). Real evidence, on the other hand, includes any physical object or material brought into court to establish or refute a pertinent fact in question (S258, Evidence Act, 2011).

[61] See (n20) supra.

[62] *Ibid*.

[63] Scientific Working Groups on Digital Evidence and Imaging Technology, 'Best Practices for Digital Evidence Laboratory Programs Glossary: version 2.7'

[64] International Organization on Computer Evidence, G8 proposed principles for the procedures relating to digital evidence (IOCE 2000). This definition has been adopted by the US Department of Justice Office of Justice Programs, National Institute of Justice, in Electronic Crime Scene Investigation: A Guide for First Responders (US Department of Justice 2001) and Forensic Examination of Digital Evidence: A Guide for law enforcement (US Department of Justice 2004).

[65] Schafer and Mason, 'The Characteristic of Electronic Evidence' in Mason and Seng (eds), Electronic Evidence (4th Edn, University of London, 2017) 19.

[66] Evidence Act 2011 recognises a "statement contained in a document produced by a computer" in s.84 (1). The phrase covers all the categorisations: electronic evidence, computer evidence, or digital evidence.

[67] See Alaba Omolaye-Ajileye, *Electronic Evidence*, (Jurist Publications Series, Lokoja, 2019) 74.

[68] See (n55) supra.

[69] See Chapter 1, Article 3 (1), Albanian Law No.9880 on Electronic Signature.

[70] https://www.adobe.com/sign/electronic-signatures.html

[71] See Part 11, Title 21 Code of Federal Regulations (CFR) that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and electronic signatures (ERES).

[72] Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, (CRC Press, 2007) 399.

[73] Section 10 (Amendment of section 258 of the 2011 Principal Act), Evidence (Amendment Act) 2023.

[74] See Section 93 (2) Evidence Act, 2011 (amended by section 4 of the Amendment Act).

[75] C.J. Michaels, MLIS, Electronic Records: Definition, Principles, and Applications, https://www.ewsolutions.com/electronic-records-definition-principles-and-applications/ accessed 5th October 2024.

[76] See n28.

[77] Philip Ukata, Electronic Records Management and National Development: A Case of Nigeria, < https://www.researchgate.net/publication/342720651_Electronic_Records_Management_and_National_Developme

nt_A_Case_of_Nigeria#:~:text=means%20any%20information%20that%20is,a%20computer%20or%20electronic% 20machine accessed 5th October 2024.

[78] Section 10 Evidence (Amendment) Act, 2023.

[79] Part 11, Title 21 Code of Federal Regulations (CFR).

[80] Section 30, Supreme Courts Ordinance, 1943.

[81] Babalola, A., *Law and Practice of Evidence in Nigeria*, (Ibadan: Sibon Books Ltd, 2001), p. 242 – 273.

[82] See s.84 of the Evidence Act, 2011.

[83] See s.84 (2) of the Evidence Act, 2011.

[84] *Faramoye v The State* (2017) LPELR – 42031(SC).

[85] *Collins Dictionary of Law*<https://legal-dictionary.thefreedictionary.com/admissibility >accessed 23 April 2024.

[86] (1984) LPELR-3259 (SC)

[87] See *Pius v The State* (2015) LPELR – 24446 (SC)

[88] (2017) 11 NWLR (Pt. 1575) 92

[89] See *Raimi v Akintoye* (1986) 3. NWLR (Pt.26) 97

[90] See (n6) supra.

[91] See (n74) supra.

[92] Section 1 of the Evidence Act 2011, sets out the exclusionary rules, which state that any evidence that is not permitted by law is considered inadmissible. This means that if such evidence is admitted, the appellate court is obligated to expunge it. This applies even if the evidence has been admitted with the consent of both parties or without objection. This principle was upheld in the court case of *Agagu v. Mimiko* (2009) ALL FWLR (pt. 462) 1122.

[93] *Udoro v Governor of Akwa Ibom State* (2016) 11 NWLR (pt. 1205) 322 at 328.

[94] See *Faramoye v The State*, (n74) supra.

[95] *R v Ellis*, (1910) 2 K.B 746, *Stirland v DPP* (1944) AC 315.

[96] See *Omidokun Owoniyi v Omotosho* (1961) 1 ALL NLR 304, (1962) WNLR 1; *Aminu v Hassan* (2014) 5 NWLR (pt. 1400) 287.

[97] See Section 251 (1) Evidence Act, 2011.

[98] https://dictionary.cambridge.org/dictionary/english/computer accessed on 23 April 2024.

[99] *Ibid.*

[100] Schafer and Mason, (n55) 20.

[101] Alaba Omolaiye-Ajileye, (n57) 99.

[102] Oxford Advance Learners Dictionary, (9th Edn, Oxford University Press 2015) 527.

[103] *R v. Daye (Arthur John)* (1908) KB 333 (KBD) 340.

[104] *Ibid*.

[105] Darling J. in *R v. Daye (Arthur John*), Ibid.

[106] Cap. E14, LFN.

[107] *Ibid.*

[108] (2003) FWLR (Pt. 145) 661.

[109] (2010) 1 NWLR (Pt. 1205) 322.

[110] Section 258 (1) Evidence Act, 2011;

[111] *Ports and Cargo Handling Services Company Ltd. & Ors. v Migfo Nigeria Ltd. & Anor.* (2012) LPELR – 9725 (SC).

[112] *Holdent International Ltd v Petersville Nigeria Ltd.* (2013) LPELR – 21474 (CA).

[113] See Section 258 (1)

[114] https://byjus.com/commerce/e-banking/#:~:text=Electronic%20banking%20has%20many%20names,different%20financial%20services%20and%20products.accessed 25 Novemebr 2024.

[115] Central Bank of Nigeria (Establishment Act) Cap. C4., 2007.

[116] Section 1 (3).

[117] Section 2.

[118] CBN Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for The Nigerian Banking Industry, 2017.

[119] See Sections 1 & 2.

[120] See Section 5 to 36.

[121] See Section 37

[122] See Section 38

[123] See Section 39

[124] Section 6 of the Act

[125] Bank and Other Financial Institutions Act, Cap. B3. Laws of Federation, 2004.

[126] Aguda O.O., "An Appraisal of the Legal Framework for Online Banking in Nigeria and South Africa" *Chukwuemeka Odumegwu Ojukwu University Journal of Commercial and Property Law,* (2021) Vol. 3(1), 11-17.

[127] See Sections 58, 59 and 60 of BOFIA.

[128] See Section 1.

[129] Section 3.

[130] Sections 31-52.

[131] Section 44 Sub-Section 1.

[132] Section 1.

[133] Section 6.

[134] See section 34

[135] See *Guaranty Trust Bank v Akinsiku Ademola* (2019) 5 NWLR (Pt. 1664) @ p. 30 (particularly at p. 43), Paras. E-H.

[136] See sections 16 and 17 Electronic Transactions Act 2011

[137] *Ibid* section 20.

[138] See Section 84

[139] See Section 85

[140] G. Omoaka and others, 'Evidence (Amendment) Act 2023: Nigerian Evidence Law Accommodates Technological Advancements',https://www.templars-law.com/app/uploads/2023/08/Evidence-Amendment-Act-2023-pdf?form=MG0AV3 accessed 8th November 2024.

[141] Section 10 of the Act (Amendment of Section 258 of the Principal Act being the Interpretation Section)

[142] Section 3 (1) of the Act (Insertion of Section 84A – 84D in the Principal Act).

[143] Section 10 of the Act (Amendment of Section 258 of the Principal Act being the Interpretation Section)

[144] Section 3(1) of the Act.

[145] Section 3(1) of the Act.

[146] Section 3 (1) of the Act (insertion of 84D (1) to the Principal Act).

[147] Section 3(1) of the Act.

[148] Such as written depositions of witnesses in judicial proceedings.

[149] A literature review of theoretical models of Internet banking adoption at the individual level | Journal of Financial Services Marketing (springer.com) accessed 6th October 2024.

[150] *Ibid.*

[151] Understanding customers' usage behavior towards online banking services: an integrated risk–benefit framework | Journal of Financial Services Marketing (springer.com) accessed 6th October 2024.

[152] Al Nahian Riyadh and Md. Shahriar Akter and Nayeema Islam, 'The Adoption of E-banking in Developing Countries: A Theoretical Model for SMEs', International Review of Business Research Papers Vol. 5 No. 6 November 2009, Pp.212-230 < https://www.researchgate.net/profile/Shahriar-Akter/publication/263848973_The_Adoption_of_E-banking_in_Developing_Countries_A_Theoretical_Model_for_SMEs/links/59dacfeea6fdcc2aad12abcf/The-Adoption-of-E-banking-in-Developing-Countries-A-Theoretical-Model-for-SMEs.pdf?form=MG0AV3>accessed 8th November 2024.

[153] A literature review of theoretical models of Internet banking adoption at the individual level | Journal of Financial Services Marketing (springer.com) accessed 6th October 2024.

[154] *Ibid*.

[155] Yousafzai S., 'A Literature Review of Theoretical Models of Internet Banking Adoption at the Individual Level', *J Financ Serv Mark* 17, 215–226 (2012). https://doi.org/10.1057/fsm.2012.19 accessed 16th November 2024.

[156] *Ibid*.

[157] Hiep, T.T.T., Thang, N.N., Thuy, P.T., Nhi, D.T.A. (2024). Exploring Determinants of E-Banking Non-adoption Among Customers: A Case Study in Export Import Commercial Joint-Stock Bank, Vietnam. In: Nguyen, N.T., Huynh, CP., Nguyen, T.T., Le-Khac, NA.,

Nguyen, QV. (eds) The 13th Conference on Information Technology and Its Applications . CITA 2024. Lecture Notes in Networks and Systems, vol 882. Springer, Cham. https://doi.org/10.1007/978-3-031-74127-2_35 accessed 8th November 2024.

[158] Kaur S., Arora S., Understanding Customers' Usage Behavior Towards Online Banking Services: An Integrated Risk–Benefit Framework. *J Financ Serv Mark* 28, 74–98 (2023). https://doi.org/10.1057/s41264-022-00140-5 accessed 1st November 2024.

[159] See (n153) supra.