Legal Analysis of Electronic Signatures in Nigeria

Hannah Olusoga-Tinubi [1]

Abstract

From 3100 B.C. when the scribe Gar Ama made his markings on a Sumerian clay tablet, through the years succeeding 1677 when the Statute of Fraud was passed into law by the British Parliament, till this present moment in 2018 , signatures were and continue to serve as a form of communication. Signatures may not only communicate the signatory's approval and adoption of the contents of a document but may also be able to authenticate the contents of a document as originating from the signatory.

Though signatures are traditionally handwritten, the giant leaps experienced in the 21st century in the field of information and communication technology have ushered in the era of the increasing use of signatures which are electronically written. The use of electronic signatures is made even more popular by stakeholders in commerce and industry who rely on technological innovations especially as it has to do with communication to facilitate commercial transactions.

Considering that laws are not made in isolation but made to respond to the needs of an ever-evolving society, several legal systems across the globe are adjusting to regulate this new and non-negligible, aspect of contract and commercial law.

1. Department of Social Justice, College of Social and Management Sciences, Afe Babalola University, Ado-Ekiti, Nigeria. hannaholusoga@gmail.com

This paper examines the place and significance of electronic signatures in the Nigerian legal system by analysing how well-adjusted the current state of laws is to the recognition and regulation of the use of electronic signatures in Nigerian commercial transactions.

Introduction

Relying on the giant strides in the field of information and communication technology, commercial transactions are increasingly being facilitated electronically. In the second quarter of 2018, the volume of electronic payment transactions in Nigeria was placed at five hundred and nine million, six hundred and sixty-eight thousand, four hundred and thirty-three (509,668,433) transactions valued at over thirty-two trillion naira (National Bureau of Statistics, 2018a). The volume of electronic payment transactions in the second quarter of 2018 represents about 11.1 percent increase in the volume of electronic payment transactions recorded in the first quarter of 2018 (National Bureau of Statistics, 2018b).

Electronic signatures form an integral part of these electronic transactions. Like the traditional handwritten signatures appended on paperbased transactions, electronic signatures seek to authenticate electronic transactions as originating from the parties to the transactions. However, unlike paper-based transactions, electronic transactions are conducted anonymously behind computer screens and are consequently more susceptible to identity fraud. Considering the volume of electronic transactions in Nigeria, the consequent use of electronic signatures in such transactions and the monetary value of these transactions, a reliable form of electronic signature which can truly authenticate the electronic transactions as originating from the parties to the transactions and an adequate legal and regulatory framework for electronic signatures are indispensable to electronic transactions.

This paper seeks to unveil how well the Nigerian legal system accommodates the concept of electronic signatures. This paper is divided into five section. The first section introduces the subject-matter. The second gives a brief summary of the history of signatures, the legal requirement of

appending signatures on certain transactions to ensure their enforceability in the courts of law, the general functions of signatures and the concept of electronic signatures and advanced electronic signatures. The significance of electronic signatures in the Nigerian legal system is considered in the third and fourth sections by elaborating on the evidentiary value of electronic signatures and the existence or inexistence of appropriate regulatory framework for advanced electronic signatures. The fifth section concludes this paper by urging that the Electronic Transactions Bill 2015 be signed into law.

Signatures

The act of signing dates back as far as 3000 BC to ancient cultures of the Sumerians (Kramer, 1963). An ancient Sumerian clay tablet dating back to around 3100 B.C. and bearing the markings of the scribe Gar Ama is one of the earliest examples of autograph signatures (Stapleton, 2014; Norman, 2018). Signatures serve the purpose of authenticating documents. It is a person's name, mark, or any other writing written by that person or at the person's direction and used with the intention of authenticating a document as originating from that person (*Black's Law Dictionary*, 2004). In modern legal history, signatures owe their wide use to the English Statute of Frauds 1677 which was an Act of the British parliament providing that for certain categories of contracts to be enforceable, they must not only be in writing but must also be signed by a party or the parties to the transaction. The categories of contract are:

1. agreements by the administrator or executor of an estate to be personally liable for the estate's liabilities;
2. agreements to answer for the debt, default or miscarriage of any other person;
3. agreements made upon consideration of marriage;
4. agreements for the sale of land or transfer of any interest in land;
5. agreements that is not to be performed within one year of its being made; and
6. agreements for the sale of goods for the price of 10 pounds and above.

It is worthy of note that in England, of these six categories of contracts indicated above, only agreements to answer for the debt, default or miscarriage of any other person; and agreements for the sale of land or transfer of any interest in land are still required to be in writing and signed by the parties to the agreement.

The Statute of Frauds 1677 is applicable in Nigeria by virtue of Section 4 of the Ordinance No. 4 of 1876 by which statutes of general application in force in England as at 1st of January, 1900 were received in to the Nigerian legal system. The reforms, in England, restricting the categories of contracts to which the Statute of Frauds, 1677 applied were introduced by statutes enacted in the years following 1st of January 1900. Therefore, the requirement for writing and signature for these six categories of contracts in the Statute of Frauds 1677 are still very much in force in Nigeria. The only exception being in eight states of the federation of Nigeria (that is Lagos, Ondo, Ogun, Osun, Oyo, Ekiti, Delta, and Edo states) who have, by local legislation, restricted the requirement for writing and signature to agreements to answer for the debt, default or miscarriage of any other person and agreements for the sale of land or transfer of any interest in land as has been done in England.

Apart from the categories of contracts referred to in the Statute of Frauds 1677, the requirement for writing and signature is necessary in Nigeria for certain transactions like the validity of wills of deceased persons, money lending agreements, bills of exchange, and promissory notes.

As stated in its preamble, the Statute of Frauds 1677 was enacted as a measure to prevent fraudulent practices which were commonly endeavoured to be upheld by perjury and subornation of perjury. Today, signatures, though widely used, are not so effective against the occurrence of fraudulent practices because signatures are easily forged and can be obtained under duress or due to misrepresentation. Hence the practice, in Nigeria, of executing (signing) certain legal instruments (for example property deeds and agreements) before third parties who serve as witnesses of due execution of the legal instruments and absence of fraud (Dadem, 2009).

Though signatures serve a variety of purposes, their legal significance is principally evidentiary. Signatures serve as evidence or proof of the identity of the signatory and evidence of the signatory's agreement with the contents

of the documents on which they appear. Mason (2016) elaborates the evidential significance or function of signatures by dividing the evidential significance into the following two categories:

1. Primary evidential function; and
2. Secondary evidential function.

The primary evidential function of a signature is to provide admissible and reliable evidence that the signatory approves and adopts the contents of the document and also agrees that the contents of the document be legally binding on him (Mason, 2016). The secondary evidential function of a signature is to serve as proof of identification of the signatory– identification of the person of the signatory, of his official status, or of the record in the document. In addition to the evidentiary significance of signatures, Mason (2016) also identifies four secondary functions of a signature which are:

1. cautionary function;
2. protective function;
3. channelling function; and
4. record keeping functions.

As a cautionary tool, signatures ensure that signatories, being aware of the legal bindingness of the document, once a signature is appended, take care not to append their signatures if there are doubts about the intent to be bound by the contents of the document. The protective function of a signature is closely linked to its cautionary function. Signatures serve as a tool of protection by inspiring a strong sense of protection and security in the parties to the agreement and others who may seek to rely on the contents of the agreement. The channelling function means that the very act of signing a document marks the point at which the document becomes legally binding. As a mark made on a document and forming an integral part of a document, signatures perform record-keeping functions by being veritable means of maintaining the history of an activity or dealing.

Electronic Signatures

Electronic signatures are comparable to handwritten signatures. They both carry out the same functions. Just like handwritten signature, electronic signature allows a signatory to leave his mark on a document with the

intention of authenticating a document as originating from him. An electronic signature may be defined as an electronic symbol, sound, or process that is either attached to or logically associated with a document and executed or adopted by a person with the intent to sign the document (*Black Law Dictionary*, 2004). Examples of electronic signatures include a clickable button ("I agree" or "I accept") on a website; a biometric hand signature signed on a special computer device; a digital or scanned image of a handwritten ink signature attached to a document; a name written at the end of an email; a signature created on a tablet device using either the finger or a stylus; a video signature; or a voice signature.

Though electronic signatures owe their existence and popularity to the giant leaps in information and communication technology as witnessed in this twenty-first century, the origin of the use of electronic and digital signatures can however be traced to the recognition of electric telegraph signatures by Common Law jurisdictions in the nineteenth century. A telegraph was, and still is, a system for sending messages over long distances by means of electric device or radio signals (Telegraph, n.d.). It allowed for communication without exchanging a tangible object (e.g. letters) containing the message. It was quite popular in the 1800s before the invention of computers and telephones. Even with the invention of telephones, telegraphs were still very much in use in the 1900s. The use of telegraphs in sending messages involved the development of a code known as the Morse code. With the Morse code, each letter in the alphabets and numbers were assigned a set of dots or dashes. These dots and dashes are represented by a series of short and long tones which were sent by electric pulses. Upon hearing the short and long tones, the telegraph operator is able to decipher the set of dots and dashes which he could then translate into English language or any other language (Telegraph, n.d.).

When a message is sent via telegraph, the signature on the document delivered to the recipient of the message is, in reality, not that of the sender but that of the telegraph operator. This is so since the message is originally a series of codes which the telegraph operator, upon receipt, must decipher, translate and then document. It is therefore quite easy to come up with legal arguments against the authenticity of the document or its contents because of the absence of the signature of the person from whom the

contents of the document originate. Such legal arguments came up in the New Hampshire case of *Howley v. Whipple* (1869), the English cases of *Godwin v. Francis* (1870), and *McBlain v. Cross* (1871). In upholding the validity and enforceability of agreements made via the telegraph, the court in *Howley v. Whipple* (1869) held that ""t makes no difference whether [the telegraph] operator writes with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. Nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office." In *Godwin v. Francis* (1870) and *McBlain v. Cross* (1871), it was held that a telegram written out and signed by a telegraph clerk on the authority of the sender was sufficient signature within the meaning of the Statute of Frauds. Just like telegraph signatures, fax signed signatures have also been declared by most common law courts to be valid.

Notwithstanding the increasing popularity of electronic signatures, Srivastava (2009) has been able to show that there are fears in the Australian business community concerning the security of electronic signatures. One cannot but wonder the justification for these fears since handwritten signatures just like electronic signatures are susceptible to forgery. The paper documents on which handwritten signatures are appended are equally, just like their electronic counterparts, susceptible to interception and alteration. The study carried out by Srivastava however shows that the fears expressed may not be unconnected to the lack of understanding of the nature, function and use of electronic signatures. In addition, the fears expressed about electronic signatures may be explained considering the fact that transactions requiring electronic signatures involve the use of computers and internet which are not so easily trusted and are usually not face-to-face transactions but rather done over a distance.

In Nigeria, just as it is the case in other jurisdictions, anonymity is the bane of electronic transactions. Anonymity tends to create hesitancy in the disclosure of personal information and financial details and provides a measure of cover for unscrupulous persons intent on mischief (Aniaka, n.d.). Compared to traditional handwritten signatures, electronic signatures are more susceptible to being used maliciously without authorisation. The

effect of such unauthorised use is to defeat the use of electronic signatures as means of establishing the identity of a party to a transaction and his approval and adoption of the contents of the documents on which his signature is affixed. Hence the development of advanced electronic signatures.

Advanced Electronic Signatures

Advanced electronic signatures are also known as digital signatures. While it is not uncommon for language users to use electronic signatures and digital signatures interchangeably, the duo are distinct and do not necessarily mean the same thing. All digital signatures are electronic signatures but not all electronic signatures are digital signatures. A digital signature is a secure, digital code attached to an electronically transmitted message that uniquely identifies and authenticates the sender (*Black Law Dictionary*, 2004). It is a code that is added to an electronic file that proves that it was created by a particular person and that it has not been changed (*Oxford Learner's Dictionary Online*, n.d.). It is a technology which makes use of cryptographic mechanism and allows two parties to validate the authenticity of electronically transmitted information and documents (Grupe, Kerr & Kuechler, 2003). The European Union Regulation Council Regulation (EU) 910/2014 of 23 July, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73 (eIDAS) defines advanced electronic signature as signature which is:

1. uniquely linked to the signatory;
2. capable of identifying the signatory
3. created using electronic signature data that the signatory can, with a high level of confidence, use under his sole control; and
4. linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Sensitive electronic transactions, like electronic fund transfers, require a reliable means of identity authentication which can only be provided by advanced electronic signatures (Okereke and Ewugwu, 2014). Advanced electronic signatures are used by large multi-national organisations and the banking industry for online banking transactions (Campbell, 2000).

Digital signatures are able to authenticate the identity of the signatory and ensure the integrity of the contents of the electronic document to which they are attached. Authentication of identity and data integrity therefore ensures that a signatory does not falsely deny appending his signature to an electronic document. Thus, contrary to views expressed by Saulawa and Marshal (2015), electronic signatures, in their basic form without the use of cryptographic mechanism, do not ensure data integrity.

The use of digital signatures requires that each signatory obtain a unique electronic key which is a pair made up of a public key and a private key. The public key, which may be made available to whosoever needs it, is used to decrypt documents to which the private key has been attached. The private key, which must not be shared, is used to encrypt documents which can only be decrypted with the public key. In addition to obtaining a unique electronic key pair, each signatory is also required to obtain a certificate validating the key pair from a trust service provider or certification authority. Note that while the digital signature authenticates the contents of the documents to which it has been attached, the digital signature certificate authenticates the identity of the digital signatory because the digital signature certificate invariably links the identity of an individual or device with a unique pair of electronic keys.

It is worthy of note that advanced electronic signature is not entirely fool-proof. Its efficacy greatly relies on the ability of the signatory to secure his private key by keeping it secret. Nevertheless advanced electronic signature is useful in reducing fund loss and damage to reputation which may be occasioned by fraud perpetrated through identity theft. It is also useful in promoting the legal enforceability of electronic transactions, protecting confidential information and avoiding the corruption or alteration of electronic data.

Admissibility of Electronic Signatures in Nigeria

The admissibility of electronic signatures refers to the acceptance or rejection of electronic signatures to prove or disprove the facts of a case in a hearing, trial or any other judicial or quasi-judicial proceeding. The admissibility of electronic and digital signatures is an area of law governed by the rules of evidence and the major source of the rules of evidence in Nigeria is the Evidence Act, 2011.

The Evidence Act, 2011, has its roots in Section 4 of the Ordinance No. 4 of 1876 by which the Common Law of England, the English Doctrine of Equity and the Statutes of General Application in force in England as at 1st of January 1900 were received into Nigeria (Babalola, 2001). The received English Law of Evidence governed the rules of evidence until 1945 when the Evidence Ordinance enacted in 1943 took effect. From 1945 till 2011, the Evidence Ordinance, later rechristened the Evidence Act, retained its contents and character without any substantial amendment. In 2011, a new Evidence Act was enacted to reflect the technological advancements of an evolving society.

Evidence adduced in a judicial proceedings may be classified in multiple ways. One of such classifications is classifying evidence as oral or documentary evidence. Documentary evidence refers to evidence furnished in writing. Most legal scholars and jurists of this age would readily agree that writings include computer-generated writings which should be considered as documentary evidence. The admissibility of computergenerated evidence however led to much uncertainty and debates in court proceedings because of the seemingly narrow legal definition given to the concept of "document" under the old Evidence Act. The old Evidence Act defines "document" to include 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 one of these means, intended to be used or which may be used for the purpose of recording that matter. Also, as noted by Oserogho and Associates (2012), computergenerated evidence was argued to offend some of the following general rules of evidence:

i. The issue of the custody and the reliability of the evidence tendered if it is not the original document;
ii. The best evidence rule which requires that a party must produce the original document during a trial or where the original document is not available, secondary evidence of it in the form of a copy, with other corroborating notes, etc, must be produced; and
iii. The rule against the admission of hear-say evidence which forbids witnesses giving evidence on facts that they do not directly or personally witness or know about.

This was the situation, even though as far back as 1969, in *Esso West Africa Inc v. T. Oyegbola* (1969) , the Supreme Court while recognising the place of computer technology in contractual and commercial relations remarked that "the law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer." In this 1969 case, one of the crucial issues which the Supreme Court had to decide was the admissibility of computer print-outs in the light of the provisions of Section 37 of the old Evidence Act which deals with the admissibility of records entered in books of accounts. According to Osinbajo (2001), Section 37 of the old Evidence Act appeared to envisage a situation where the entries must be made in an existing book or bound volume specifically designated as "Book of Account" and this definition would hardly admit a computer print-out of a customer's statement of account. The Supreme Court's liberal approach in not limiting the interpretation of Section 37 to bound books of account with pages not easily replaced is therefore commendable. It is worthy of note that Section 37 of the old Evidence Act is now contained in Section 51 of the Evidence Act 2011 and has been re-enacted to expressly allow for the admissibility of electronic records.

Notwithstanding the Supreme Court's liberal interpretation of the provisions of the law to reflect advancements in the field of computer technology, the admissibility of computer-generated evidence continued to generate controversies especially at trial courts so much that there was the need to amend the Evidence Act and this was done with the enactment of the Evidence Act in 2011 which repeals the old Evidence Act and applies to all judicial proceedings in or before courts in Nigeria. One of the significant changes in the 2011 Act is the expansion of the general rules of evidence to expressly allow for the admissibility of electronically generated evidence.

Section 93, Sub-Section 2 of the Evidence Act 2011 provides that "where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences." The implication of this provision of the Evidence Act 2011 is to allow for the admissibility of electronic signatures in all situations where handwritten signatures are admissible. The admissibility of electronic signatures was further affirmed by the legislature in 2015 when the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 was

enacted into law. Section 17 of the Act explicitly provides that "electronic signature in respect of purchases of goods, and any other transactions shall be binding."

However, the legislature, by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, limits the admissibility of electronic signatures by excluding certain transactions from the categories of contractual transactions or declarations that are valid by virtue of electronic signature. The transactions are:

1. Creation and execution of wills, codicils and or other testamentary documents;
2. Death certificate;
3. Birth certificate;
4. Matters of family law such as marriage, divorce, adoption and other related issues;
5. Issuance of court orders, notices, official court documents such as affidavit, pleadings, motions and other related judicial documents and instruments;
6. Any cancellation or termination of utility services;
7. Any instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; and
8. Any document ordering withdrawal of drugs, chemicals and any other material, either on the ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.

Also worthy of mention is the provision of Section 93, Sub-Section 3 of the Evidence Act 2011 which provides that "all electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person."

Though, neither Section 93 of the Evidence Act 2011 nor any other provision of the Evidence Act 2011 makes use of the word "digital signature" or "advanced electronic signature," the implication of the above stated provisions of Section 93 of the Evidence Act 2011 is to allow for the

admissibility of digital signatures which, as explained in the preceding pages, involve a procedure by which a symbol or security procedure is executed to authenticate the identity of the signatory of an electronic record or transaction. Note also that whenever the genuineness or otherwise of electronic signatures is in question, the burden of proof, that the electronic signature does not belong to the purported originator of such electronic signatures shall be on the contender.

Unfortunately, though electronic signatures are commonly used in the private sector and by governmental agencies in the performance of their statutory duties, nether the Evidence Act 2011 nor the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 gives a definition of electronic signatures or advanced electronic signatures. It is nevertheless comforting that notwithstanding the absence of a definition or judicial authority as to what constitutes electronic or digital signature, courts are not left in the dark as they can rely on the judicial decisions in other jurisdictions which, though not binding on the courts, are of persuasive authority.

Regulatory Framework for Advanced Electronic Signatures

While it might be enough for the legal system to simply provide for the admissibility of electronic signatures, same cannot be said for advanced electronic signatures. A regulatory framework is a necessity for advanced electronic signatures.

It was previously mentioned in this paper that in order for signatories to make use of advanced electronic signatures, each signatory must obtain a unique electronic key pair and a certificate validating the key pair from a trust service provider or certification authority. It was explained that while the digital signature authenticates the contents of the documents to which it has been attached, the digital signature certificate issued by a trust service provider or certification authority authenticates the identity of the digital signatory. The certification authority is therefore in the business of giving assurance to the signatories to conduct their electronic transactions using the advanced electronic signatures certified by the certification authority.

If the digital signature authenticates the contents of the documents to which it has been attached and the digital signature certificate issued by a trust service provider or certification authority authenticates the identity of

the digital signatory, who authenticates the identity of the certification authority upon whose assurance parties may proceed to conclude electronic transactions with significant financial implications? According to Biddle (1997), "the certification authority must also somehow provide assurance that it is bound to its public key, which is used to verify.... Thus, the certification authority could have its own certificate, signed with the digital signature of a 'higher level' certification authority. This higher level certification authority might be (as under some of the enacted digital signature laws) a government agency."

An adequate regulatory framework allows for the authentication of certificate authorities. It allows the national government to ensure the security of advanced electronic signatures by controlling the activities of trust service providers and setting out their duties, obligations and liabilities. Consequently, it would also serve the purpose of displacing the clouds of mistrust that may arise in the minds of consumers and businesses as a result of the legal uncertainty that accompanies the inexistence of a regulatory framework. As succinctly put by the European Union Parliament in the preamble of the eIDAS, 2014 "building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services." A regulatory framework for advanced electronic signatures also allows a government to establish and maintain an electronic identification scheme in its territory.

The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures serves as a guide to national governments who seek to formulate or enhance legislative and regulatory frameworks for advanced electronic signatures. The electronic signature regulatory regime of some states is a result of the policy transfer from the UNCITRAL Model Law on Electronic Signatures. The United States of America's Electronic Signatures in Global and National Commerce Act, 2000, the Indian Information Technology Act, 2000, the South African Electronic Communications and Transaction Act, 2002, and the European Union's Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July, 2014 on Electronic Identification and Trust Services

for Electronic Transactions in the Internal Market are examples of states' policy transfer from the UNCITRAL Model Law on Electronic Signatures.

In the European Union, the Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July, 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) regulates the use of electronic signature. The eIDAS Regulation was preceded by the European Union's Electronic Signature Directive 1999/93/EC on Electronic Signature which directive was repealed to make way for a regulation which not only deals with electronic signatures but also provides a comprehensive cross- border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. The eIDAS Regulation makes provision for the following:

1. Admissibility of electronic signatures in legal proceedings;
2. Regulation of certificates for electronic signature;
3. Regulation of electronic signature creation device;
4. Establishment, regulation and mutual recognition of Electronic Identification Schemes among member states; and
5. Registration, supervision, duties, obligations and liabilities of Trust services.

Note that some governments choose not to model their electronic signature regime after the UNCITRAL Model Law on Electronic Signatures. Eko and Tolstikova (2005) note that while United States of America's electronic signature regime is a result of the policy transfer from the UNCITRAL Model Law on Electronic Signatures, the Russian Federation's electronic signature regulatory regime is not a result of policy transfer from the UNCITRAL Model Law on Electronic Signatures.

National Information Technology Development Agency's Public Key Infrastructure Regulations

The National Information Technology Development Agency (NITDA) is the agency charged with the responsibility of creating a framework for the regulation of information technology practices, activities and systems in Nigeria. Pursuant to the powers derived from the National Information Technology Development Act 2007, NITDA issued the NITDA Public Key

Infrastructure (PKI) Regulations 2017 (NITDA PKI Regulations) thereby creating in Nigeria a comprehensive regulatory framework for advanced electronic signatures. The NITDA PKI Regulations 2017 confers evidentiary presumption of regularity in judicial proceedings on digital signature certificates issued by certification authorities duly licensed by NITDA. The NITDA PKI Regulations also gives conditions for limiting the liability of licensed certification authorities amongst many other provisions.

Electronic Transaction Bill 2015

The Electronic Transaction Bill 2015 is a Bill for an Act to facilitate the use of information in electronic form for conducting transactions in Nigeria and for other connected purposes. The Electronic Transactions Bill 2015 has passed through the two houses of the National Assembly but still awaits presidential assent to take effect as law. The Electronic Transaction Bill 2015 recognises that the administration of electronic signatures shall be in accordance with the rule, guideline and standards prescribed by NITDA. The objective of the Bill is to provide a legal and regulatory framework for:

1. Conducting transactions using electronic or related media;
2. The protection of the rights of consumers and other parties in electronic transactions and services;
3. The protection of personal data; and
4. Facilitating electronic commerce in Nigeria.

As it concerns electronic signatures, the Electronic Transaction Bill 2015 provides for the following:

- The validity of electronic signatures;
- The administration of electronic signatures;
- Certification authority;
- Recognition of foreign certification authority;
- Record retention by certification authority; and
- Liability of certification authority

Conclusion

The National Information Technology Development Act 2007 , the Evidence Act 2011, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and the

National Information Technology Development Agency's Public Key Infrastructure Regulations each represent a milestone achievement for the legal and regulatory framework for electronic identity authentication.

It is recognised that the letters of the NITDA Public Key Infrastructure (PKI) Regulations 2017, especially as it has to do with the licensing of certification authorities, may remain dead letters in the Regulations until NITDA in its capacity as licensing authority receives application from prospective certification authorities. This occurred in South Africa where the Department of Communications (the South African licensing authority) did not accredit a certification authority until nine years after it was empowered to license certification authorities (Eiselen, 2014).

Nevertheless, through the instrumentality of these laws and regulations, Nigeria has been able to ensure the admissibility of electronic signatures in judicial proceedings, the adequate regulation of key-players in the industry and the ultimate continued relevance of laws to the computer-driven economy.

It is strongly recommended that the Electronic Transactions Bill 2015 be passed into law to further consolidate the position of the National Information Technology Development Agency.

References

Aniaka, O. (n.d.). Analysing the adequacy of the electronic transactions bill 2015 in facilitating e-commerce in Nigeria. Retrieved from http://ssrn.com/abstract=2651120.

Babalola, A. (2001). Definition, nature, scope, classification and sources of Nigerian law of evidence. In Afe Babalola (Ed), *Law and practice of evidence in Nigeria*. Ibadan, Nigeria: Sibon Books Limited.

Biddle, B. (1997). Legislating market winners: Digital signature laws and the electronic commerce marketplace. *San Diego Law Review*, 34, 1225.

Campbell, B. (2000). Public-key infrastructure and online banking. Retrieved from https://www.giac.org/paper/gsec/223/public-key-infrastructure-onlinebanking/100732.

Dadem, Y.Y.D. (2009). *Property law practice in Nigeria*. Jos Nigeria: Jos University Press Limited.

Digital signature. (2004). *In Black's Law Dictionary* (6 th ed.). Thomson West, USA: West Publishing Co..

Digital signature. (n.d.) *In Oxford learner's dictionary online*. Retrieved from https://www.oxfordlearnersdictionaries.com/definition/english/digitalsignature?q=digital+signature.

Eiselen, S. (2014). Fiddling with the ECT Act– Electronic signatures. *Potchefstroom Electronic Law Journal*, *17*(6), 2805-2820.

Eko, L. and Tolstikova, N. (2005). To sign or not to sign on the electronic dotted line: The United States, the Russian federation, and international electronic signature policy. *International Journal of Communications Law and Policy, Special Issue Global Flow of Information* 1 - 27.

Electronic signature. (2004). *In Black's Law Dictionary* (6th ed.). Thomson West, USA: West Publishing Co.

Grupe, F. *et. al.* (2003). The CPA and the computer: Understanding digital signatures. *The CPA Journal* 70-72.

Kramer, S.N. (1963). *The Sumerians: Their history, culture and character.* Chicago: The University of Chicago Press.

Mason, S. (2016). *Electronic signatures in law*. London: Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London.

National Assembly. (2017). *Report of the Conference Committee on Electronic Transactions Bill 2017*. Nigeria. Retrieved from http://placng.org/wp/wpcontent/uploads/2017/05/Report-of-the-Conference-Committeeon-ElectronicTransactions-Bill-2017.pdf

National Bureau of Statistics. (2018a). *Selected banking sector data: Sectorial breakdown of credit, ePayment channels, and staff strength (Q2 2018)*.

Nigeria. Retrieved from http://nigerianstat.gov.ng/elibrary?page=2&offset=10

National Bureau of Statistics (2018b*) . Selected banking sector data: Sectorial breakdown of credit, ePayment channels, and staff strength (Q1 2018)*.

Nigeria. Retrieved from http://nigerianstat.gov.ng/elibrary?page=7&offset=60

Okereke, G.E. and Ezugwu, O.A. (2014). Authenticating e-banking services in Nigeria through digital signatures. *African Journal of Law and Computing* 7(3) 47-52.

Oserogho and Associates (2012, May). Admissibility of electronic evidence. Retrieved from www.oseroghoassociates.com/articles/30admissibility-ofelectronic-evidence?print=1&download=0

Osinbajo, Y. (2001). Electronically generated evidence. In Afe Babalola (Ed), *Law and practice of evidence in Nigeria*. Ibadan, Nigeria: Sibon Books Limited.

Saulawa, M.A. and Marshal, J.B. (2015). The relevance of electronic signatures in electronic transactions: An analysis of the legal framework. *Journal of Law, Policy and Globalisation 34*. 5-13.

Signature. (2004). *In Black's Law Dictionary* (6th ed.). Thomson West, USA: West Publishing Co.

Srivastava, A. (2009). Electronic signatures and security issues: An empirical study. *Computer Law and Security Review 25*. 432-446.

Stapleton, J.J. (2014). *Security without obscurity: A guide to confidentiality, authentication, and iIntegrity.* USA: CRC Press.

Telegraph. (n.d.). *In Collins Dictionary online.* Retrieved from https://www.collinsdictionary.com/dictionary/english/telegraph;

Telegraph. (n.d.). *In Dictionary.com.* Retrieved from http://www.dictionary.com/browse/telegraph;

Telegraph. (n.d.). *In History of Information*. Retrieved from http://www.historyofinformation.com/expanded.php?id=2614

Cases

Chua Sock Chen v. Lau Wai Ming [1989] SLR 1119

Esso West Africa Inc v. T. Oyegbola (1969) 1 NMLR 194

Festus Sunmola Yesufu v. ACB 1976 4 SC 1

Godwin v. Francis (1870) LR 5 CP 295

Goodman v. J Eban Ltd [1954] 1 All E.R. 763

Holdent International Ltd v. Petersville Nigeria Ltd (2013) LPELR – 21474 (CA)

Howley v. Whipple 48 N.H. 487

McBlain v. Cross (1871) 25 LT 804

Molodysky v. Vema Australia Pty Ltd [1989] AUConstrLawNlr 14

Obatuga & Anor v. Oyebokun & Ors (2014) LPELR 22344 (CA)

Polythecnic Ede & Ors v. Oyebanji (2012) LPELR 19696 (CA

Ports and Cargo Handling Services Company Ltd v. Migfo Nigeria Ltd (2012) 18 NWLR [Pt. 1333] 555 S.C. at 593

Re United Canso Oil & Gas Ltd (1980) 12 B.L.R. 130

Standard Bank London Ltd v. Bank of Tokyo Ltd [1995] CLC 496