DEFINING THE SCOPE AND APPLICATION OF THE LEGALITY OF ELECTRONIC SIGNATURE IN NIGERIA

Written by ***James Agbadufishim***

Former Senior Lecturer, Faculty of Law, University of Abuja and Judge, National Industrial Court of Nigeria, Nigeria

ABSTRACT

Since the emergence of e-commerce in the nineties, security has become a significant barrier to its growth. Businesses and individuals involved in e-commerce must be able to place their trust and confidence in the identity of the other party, as well as in the integrity of any electronic messages received, to ensure that they have not been altered.

Identification and authentication via an electronic signature provide both parties with assurances concerning the identity and the integrity of the message. From a legal perspective, the role of legislation in this context is to offer the necessary guarantees of a secure and trustworthy online transaction. This can be achieved through the recognition of electronic signatures and regulating the certification of service providers.

This paper will consider the different forms of electronic signatures which exist, and the present legislation in Nigeria which deals with their recognition. It will also examine the legal effects and the adequacy of the present legal framework. Finally, it will conclude by discussing how the legislature in Nigeria can improve the present framework to meet the current international legal and technological standards which would enhance the validity and enforceability of electronic contracts that have been executed using electronic signatures by parties within Nigeria.

Keywords: Electronic Signature, Digital Signature, Law of Contract, Electronic Contract, Electronic Commerce

INTRODUCTION

Although e-commerce presents many possibilities, it is characterized by users' lack of confidence in its e-transactions as a result of, among others the anonymity of Internet users. While contracting online, parties to an e-transaction need to know that the person sitting at a keyboard transacting with them is whom they say they are and has authority to act.[i] A party's ability to assent to contracts through electronic means constitutes one of the main concerns in e-transactions so that the parties know they have reached a binding agreement.[ii]

Consequently, e-commerce users have to adopt a secure means to address these concerns in an almost similar manner to traditional contracts. This is done through the use of "electronic signatures" in online or electronic contracts.

Electronic signatures are generally similar to traditional signatures in their purpose in a contract – which is to authenticate and validate a contractual relationship or agreement.[iii] The word 'signature' comes from the Latin word '*signare*', which means 'to sign or mark'. The Random House Unabridged Dictionary defines 'signature' as a 'person's name, or a mark representing it, as signed personally, as in subscribing a letter or other document'. It also defines 'signature' as 'the act of signing a document'. Webster's Dictionary defines 'signature' as 'the name of one as written by oneself'.

Signatures in a contract are important and well recognised in contract law, though very little is written about traditional signatures. Traditional signatures are mainly used as evidence and they are verified only in case of a dispute. Hence, traditional signatures have forensic value and evidential value.

Generally, as stated numerously in this common law cases, most contracts are devoid of formalities and could be concluded in writing or orally and completed either electronically or physically. The informal contracts, which included contracts of sale and lease could be concluded safely over the Internet. Many contracts were required to be in writing or had some other formal requirements, such as the attachment of a physical signature or attestation by witnesses to be effective. However, these formal requirements caused problems when the principles of electronic contracting were applied.[iv] The main issue is the application of the traditional contract rules or requirement in cyberspace, which necessitate that the contracts formed or concluded online to be 'written' or be 'in writing'. The other issue is whether a digital document could fulfil the necessary formal requirements of such contracts.[v]

SIGNATURES AND FORMATION OF ENFORCEABLE CONTRACTS

When there was a requirement for writing in a contract, then reference was usually made to the Nigerian Interpretation Act[vi], which defined writing as:

> including typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form.

The above definition of writing meant that for many formal contracts, electronic contracting could not be used as digital communication. A series of electrical impulses did not have the requisite degree of visibility that was required by the definition under the Interpretation Act. Different forms of traditional signatures, such as rubber stand, telex signature, faxed copy, printed name, handwritten signatures were recognised as valid under various English cases.[vii] A very famous case of *Lobb v Stanley*[viii] where the issue of signature was somewhat exhaustively discussed by the court. The court recognized the importance of affixing the name of a party as a signature and stated that a signature was only a mark, and held that even the printed name of the party who was required to sign the document was sufficient to be considered a signature. In this case, the Justices, Lord *Denham CJ, and Patterson, Coleridge and WrightmanJJ*, argued as to what could be construed as a signature. The facts of the case were that Stanley, a certified bankrupt gave a signed, written promise following the bankruptcy. Out of the three undated letters, which were produced by Stanley, one of the letters read that:

> Mr Stanley begs to inform MrLobb that he will be glad to give him a promissory note or bill for the amount of Mr Stanley's account, payable at three months, as Mr Stanley has of late been put to heavy expenses, and hopes this arrangement will be satisfactory to MrLobb. 3 Crescent. Thursday morning.

In his judgment, Patterson J stated:

> It is true that the word 'signed' occurs in the statute and if this had been the first time that we were called upon to put a construction on that word, and if the decisions on the Statute of Frauds had not occurred, I should perhaps be slow to say that this was a signature.[ix]

Although Lord Denham CJ agreed that the letters were not signed in one sense, the intrinsic evidence of the documents proved the signature. He pointed out that:

> It is a signature of the party when he authenticates the instrument by writing his name in the body, Here; it is true the whole name is not written, but only 'Mr Stanley'. I think more is not necessary.

Finally, it was unanimously agreed that Stanley signed the documents, Stanley wrote the letters himself and he identified himself by surname in the body of the letters. By identifying himself in this manner, Stanley demonstrated that he intended the recipient to rely on the promise contained in the letter. Thus, the signature was his assertion because he wrote his surname and he intended that the content of the letters were to be acted upon by the recipient.

This, therefore, brings us to the modern times with the following question – can the decision of the court in *Lobb v. Stanley* be valid in electronic contracts or agreements with regards to "signature" of a party? Although in traditional cases, different types of signatures were considered valid, attribution of the message to a particular sender was considered a matter of concern, as there was no clear authority dealing with the issue. Hence, the requirement of signature was also considered problematic.[x] A signature is a process. If that process produces sufficient evidence indicating that a person has adopted a document as his own and if that document appears to be the same document to which the process is applied, then the document can be considered signed. It is not relevant whether the result of that process is a visible mark or a symbol. So in one way, it can be said that a signature is evidence.[xi] Unlike traditional signatures, which can be attributed to a person, electronic signatures cannot create evidence, as they can be easily tampered with and suffer from limitations.[xii]

In Nigeria, the function of a traditional signature is effected by any method and the ordinary meaning of a signature is nothing but a mark in a written document.[xiii] Signatures are important in a document and traditional signatures are not only important in a paper-based document but they are also used for the evidential purpose in a contract.[xiv] There are four historical policy objectives for the requirements of writing and signatures, which include evidentiary, cautionary, channelling and record keeping.[xv] Though these functions are not discreet, they are intimately connected. The requirement of a signature has a protective effect since it cautions the signatory. Further, the need for a signature can also warn the signer or signatory that the document has legal consequences and encourage the signatory to think whether he or she wants to be legally bound by affixing the signature. This function is considered an important issue in protecting consumers.[xvi]

As noted earlier, a "signature" is "any name or symbol used by a party to constitute it his signature".[xvii] It is understood that the purpose of statutes that require a particular document to be signed by a particular person is to confirm the genuineness of the document.[xviii] The paradigm case of signature is the signatory's name, written in the signatory's hand, on a paper document (a "handwritten" or "manuscript" signature). Lord Denning in *Goodman v. Eban*[xix]:

> In modern English usage when a document is required to be signed by someone that means that he must write his name with his own hand upon it.

However, the handwritten signature is not the only conceivable type of signature. Since courts regard signatures as "only a mark" unless the statute in question requires the signature to be an autograph, "the printed name of the party who is required to sign the document is enough", or the signature "may be impressed upon the document by a stamp engraved with a facsimile of the ordinary signature of the person signing", provided that proof in these cases is given "that the name printed on the stamp was affixed by the person signing", or that such signature "has been recognized and brought home to him as having been done by his authority to appropriate it to the particular instrument".[xx]

Legal signature requirements as a condition for the validity of certain acts in common law jurisdictions are typically found in the British Statute of Frauds[xxi] Most of its provisions were repealed in the United Kingdom during the twentieth century. With time, courts have tended to interpret the Statute of Frauds liberally, out of the recognition that its strict form requirements were conceived against a particular background and that strict adherence to its rules might unnecessarily deprive contracts of legal effect. As explained by Lord Bingham of Cornhill in *Actionstrength Limited v. International Glass Engineering*[xxii]:

> It quickly became evident that if the seventeenth-century solution addressed one mischief it was capable of giving rise to another: that a party, making and acting on what was thought to be a binding oral agreement, would find his commercial expectations defeated when the time for enforcement came and the other party successfully relied on the lack of a written memorandum or note of the agreement.

Furthermore, Roxborough J. in *Leeman v. Stocks*[xxiii] noted that:

> The Statute of Frauds was passed at a period when the legislature was somewhat inclined to provide that cases should be decided according to fixed rules rather than to leave it to the jury to consider the effect of the evidence in each case. This, no doubt, arose to a certain extent from the fact that in those days the plaintiff and the defendant were not competent witnesses.

Thus, in the last 150 years, common law jurisdictions have seen an evolution of the concept of "signature" from an original emphasis on the form to a focus on function. Variations on this theme have been considered by the English courts from time to time, ranging from simple modifications such as crosses[xxiv] or initials[xxv] to pseudonyms[xxvi] and identifying phrases,[xxvii] to printed names,[xxviii] signatures by third parties[xxix] and rubber stamps.[xxx] In all these cases the courts have been able to resolve the question as to whether a valid signature was made by drawing an analogy with a manuscript signature. Thus, it could be said that against a background of some rigid general form requirements, courts in common law jurisdictions have tended to develop a broad understanding of what the notions of "authentication" and "signature" mean, focusing on the intention of the parties, rather than on the form of their acts.

NATURE AND LEGAL ELEMENTS OF ELECTRONIC SIGNATURE

Electronic documents and transactions need to be signed just as paper documents do. The effect of an e-signature in an e-transaction needs to be similar to that of a traditional signature in the offline world. This is because it is important to verify that the person sitting at a keyboard is who he/she claims to be, and is authorised to perform the act he/she asserts is authorized to do.[xxxi]

Information and computer technology have developed various means for linking information in the electronic form to particular persons or entities, for ensuring the integrity of such information or for enabling persons to demonstrate their entitlement or authorization to obtain access to a certain service or repository of information. These functions are sometimes referred to generically either as electronic "authentication" or electronic "signature" methods. Sometimes, however, distinctions are made between electronic "authentication" and electronic "signature". The use of terminology is not only inconsistent but is to some extent misleading. In a paper-based environment, the words "authentication" and "signature" and the related

actions of "authenticating" and "signing" do not have the same connotation in different legal systems and have functionalities that may not necessarily correspond to the purpose and function of the so-called electronic "authentication" and "signature" methods.

Researchers on digital security and authentication have made several attempts to define the concept of "e-signature" over the years. For one, an e-signature is defined as 'anything in electronic form that can be used to demonstrate a signing entity intended their signature to have legal effect.'[xxxii] It is also described as 'any symbol, mark or method, accomplished by electronic means, executed by a party with the present intent to be bound by a record or to authenticate a record.'[xxxiii] The words 'electronic signature' therefore signifies the general concept of a signature, which is conveyed by the application of a computer or computer-like device.[xxxiv]

An electronic signature is a term often used to describe 'signatures', which are affixed or incorporated in electronic contracts or documents through electronic or cryptographic means. Some of the examples of electronic signatures include insertion of a scanned version of the signatory or signer's signature in an electronic transaction or typewritten name of the signer or signatory at the end of an email or electronic communication or using cryptographic technology such as a digital signature or a person clicking 'I accept' button and the use of a password.[xxxv] Electronic signatures may function in the same way as a handwritten signature, by identifying the person who has affixed or appended the signature to the electronic communication or document and may indicate the willingness and agreement of the signatory regarding the content of the electronic document. However, in most of the examples of electronic signatures identified above (except digital signature), the sender's identity and the integrity of documents cannot be established.[xxxvi]

The terms "electronic signature", "digital signature", "digital authentication" and, increasingly, "digital identity" are sometimes used interchangeably; however, they do not mean the same thing. An electronic signature (e-signature) is a process of signalling intent, including acceptance, as to the content of an electronic record.[xxxvii] Practically speaking, the technologies used for e-signatures include email addresses, enterprise IDs, personal ID numbers (PINs), biometric identification, social IDs, scanned copies of handwritten signatures and clickable "I accept" boxes.[xxxviii]

A digital signature, or advanced e-signature, uses cryptography to scramble signed information into an unreadable format and decodes it again for the recipient. Specialized third parties,

known as certification authorities (CAs), often provide certification services for verifying the signer's identity. In certain instances, some firms may choose to use their systems.[xxxix]

Some jurisdictions, such as the European Union (EU), distinguish between digital signatures and qualified e-signatures (or qualified digital signatures). While both rely on encryption and CAs to identify the signer, the qualified e-signatures also require the signer to use a qualified signature creation device (QSCD), such as a smart card, token or cloud-based trust service. The QSCD verifies the digital identity and can only be given to users once they have passed a Know-Your-Customer (KYC) process.

Scholars make a distinction between signature as a legal term and signature as a technical term in e-communications.[xl] Some maintain that signature as a legal term refers to any e-signature technology that can work in place of a manuscript signature in e-transactions and have a legally binding effect, while signature as a technical term refers to a digital signature supported by Public Key Infrastructure (PKI) technology.[xli] This distinction gives two different implications on the use of e-signatures.[xlii] That is, a technical signature ensures the integrity and authentication of signed data.[xliii] Hence it is a technology that provides information security. Mason suggests that authentication in the context of information security has two meanings relevant to e-signatures. First, it refers to the verification of the identity of a person and secondly, refers to verification of the origin of a message. Thus some scholars maintain that an e-signature is not a signature per se, but 'just authentication technologies used to confirm the origin of a document.'[xliv] On the other hand, the legal notion of e-signature attempts to equate an e-signature to a handwritten signature that reflects a signer's assent to information.[xlv]

However, Sjoberg and Norden argue that different views of e-signature as a legal or technical term cause confusion as users tend to forget that a signature is not just a legal notion but sometimes predominantly serves to safeguard the integrity of a document in e-communication.[xlvi] As a result, they find it prudent to use the term 'e-signature' as a synonym of the digital signature, yet careful to explicitly mention the digital signature where the need arises.

On the contrary, other researchers adopt a broad meaning of technical signature. They maintain that technical signature as 'any action that utilises Information and Communications Technology and is recognised as a signature in a law.'[xlvii] The latter term, therefore, includes both e-signatures used for identification and the digital signature.

Despite the proposed differences between legal and technical signature, this study adopts Sjoberg and Norden's views. It understands that an e-signature is any technology that uses ICT in e-transactions to show a party's assent to information (authentication) and sometimes show the integrity of a message.[xlviii] Hence 'e-signature' in this work encompasses all e-signature technologies including the digital signature supported by PKI. Put differently, a digital signature based on PKI is a form of e-signature, but an e-signature may consist of other technologies apart from the digital signatures based on PKI. Amongst these technologies are the username, passwords, electronic sound, typed name in an e-document, clicking on an icon, acceptance through browse wrap agreements, email signature, digitised signature, contactless identification, biometrics technology and digital signature based on a Pretty Good Privacy (PGP) web of trust. Although the digitised signature sounds like the digital signature, the two are different forms of e-signatures.

Neither the UNCITRAL Model Law on Electronic Commerce nor the UNCITRAL Model Law on Electronic Signatures uses the term "electronic authentication", because of the different meaning of "authentication" in various legal systems and the possible confusion with particular procedures or form requirements. The Model Law on Electronic Commerce uses instead the notion of "original form" to provide the criteria for the functional equivalence of "authentic" electronic information. According to article 8 of the Model Law, where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) There exists "a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) Where it is required that information be presented, that information "is capable of being displayed to the person to whom it is to be presented.

In keeping with the distinction made in most legal systems between signature (or seals, where they are used instead) as a means of "authentication", on the one hand, and "authenticity" as the quality of a document or record on the other, both model laws complement the notion of "originality" with the notion of "signature". Article 2, subparagraph (a), of the UNCITRAL Model Law on Electronic Signatures defines an electronic signature as data in electronic form in, affixed to or logically associated with, a data message, which may be used to "identify the signatory" in relation to the data message and to "indicate the signatory's approval of the information contained in the data message".

The definition of "electronic signature" in UNCITRAL texts is deliberately broad, to encompass all existing or future "electronic signature" methods. As long as the methods used are "as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement", they should be regarded as meeting legal signature requirements.

The UNCITRAL model laws do not deal otherwise with issues related to access control or identity verification. This was also in keeping with the fact that, in a paper-based environment, signatures may be signs of identity but are necessarily attributive of identity. The UNCITRAL Model Law on Electronic Commerce deals, however, with the conditions under which the addressee of a data message is entitled to assume that the message originated from its purported originator. Indeed, article 13 of the Model Law provides that as between the originator and the addressee, a data message is deemed to be that of the originator if it was sent by a person "who had the authority to act on behalf of the originator in respect of that data message" or by "an information system programmed by, or on behalf of, the originator to operate automatically".

Several different electronic signature techniques have been developed over the years. Each technique aims at satisfying different needs and providing different levels of security and entails different technical requirements. Electronic authentication and signature methods may be classified in three categories: those based on the knowledge of the user or the recipient (e.g. passwords, personal identification numbers (PINs)), those based on the physical features of the user (e.g. biometrics) and those based on the possession of an object by the user (e.g. codes or other information stored on a magnetic card).[xlix]

A fourth category might include various types of authentication and signature methods that, without falling under any of the above categories, might also be used to indicate the originator of electronic communication (such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message). Technologies currently in use include digital signatures within a public key infrastructure (PKI), biometric devices, PINs, user-defined or assigned passwords, scanned handwritten signatures, signature utilizing a digital pen, and clickable "OK" or "I accept" boxes.[l]

Interestingly, in Nigeria, the requirement of a signature can be satisfied in the case of electronic documents by an electronic signature, by typing a name into an electronic document or even by clicking on a website button. This is buttressed by Section 93(2) of the Nigerian Evidence Act 2011, which reads:

> Where a rule of evidence requires a signature or provides for certain consequences if the document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.

Section 93(3) goes further:

> All electronic signatures 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.

Furthermore, Section 17 of the Cybercrimes (Prohibition and Prevention) Act, 2015 also recognizes the use of electronic signatures in Nigeria, they are court-admissible and safe for general business use. It provides that electronic signature in respect of the purchase of goods, and any other transactions shall be binding. It, however, excludes certain transactions from the categories of valid contractual transactions using electronic signatures such as creation and execution of wills, codicils and other testamentary documents, death and birth certificates, matters of family law such as marriage, divorce, adoption and other related issues etc.

Lastly, it ought to be pointed out that there is a huge difference between electronic signatures and email signatures. An email signature authenticates a document. Email signature refers to either the name in an email address or an email signature block.[li] The information that appears on the 'From' line in an email, which is an email address, clearly indicates who the sender of an email message is and identifies them as the signer of the message. Hence it constitutes a signature.[lii]Chissick argues that an email address can be compared to a traditional signature in two ways. Firstly, the signer's act of clicking on the send button is equated to the signature of a hard copy document by attachment of a stamp. Secondly, the email address is equated to a letterhead on an offline letter, which indicates who the communication is from.[liii]

An email signature block on the other hand is a collection of text located at the bottom of an email message. The block consists of the name of a sender and their contact details. The email block is attached to every email a sender sends to their receivers as a form of identification.[liv] The shortcoming of such email footer is that an imposter can easily forge it by copying and pasting it where he/she wants, or they can just type in the contents of the email footer at the

end of a message.[lv] A fraudster may also use another person's email to defraud others or send defamatory content.

ELECTRONIC SIGNATURE AND DIGITAL AUTHENTICATION

Digital authentication refers variously to the techniques used to identify individuals, confirm a person's authority or prerogative, or offer assurance on the integrity of information. "Authentication" can mean different things in different national legal contexts, with the challenge of doing it remotely over networks.[lvi] Digital authentication can rely on a varied set of factors, such as those concerning knowledge (e.g. passwords, answers to a pre-selected security question), ownership (e.g. possession of a one-time password) or inherence (e.g. biometric information). Depending on the level of security desired, a digital authentication system could be single-, double- or multi-factor.[lvii]

The notions of "authentication" and "authenticity" are generally understood in law to refer to the genuineness of a document or record, that is, that the document is the "original" support of the information it contains, in the form, it was recorded and without any alteration. Signatures, in turn, perform three main functions in the paper-based environment: signatures make it possible to identify the signatory (identification function); signatures provide certainty as to the personal involvement of that person in the act of signing (evidentiary function), and signatures associate the signatory with the content of a document (attribution function). Signatures can be said to perform various other functions as well, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might flow from the act of signing); the intent of a person to associate him or herself with the content of a document written by someone else; and the fact that, and the time when a person has been at a given place.[lviii]

It should be noted, however, that even though authenticity is often presumed by the existence of a signature, a signature alone does not "authenticate" a document. The two elements may even be separable, depending on the circumstances. A signature may retain its "authenticity" even though the document to which it is affixed is subsequently altered. Likewise, a document may still be "authentic" even though a signature it contains was forged.

Digital identity refers to a broader conception of the information used by a computer system to identify an agent, which is most frequently considered to be an individual but is also referred to as an entity, such as a corporation or a machine. Printed documents such as passports, national ID cards and driver's licences offer proof of a person's identity. Similarly, online electronic information can be linked to an individual or another entity to offer proof of identity.[lix]

It has been argued that traditional witnessing processes, such as attestation, which may be used in connection with, but also independently from, the drawing up of a public deed by a notary public, are not wholly adaptable to the process of electronically signing documents, since there is no assurance that the image on the screen is, in fact, the document to which the electronic signature will be affixed. All that the witness and the signatory can see is a representation on the screen, capable of being read by a human being, of what is allegedly in the information system. When the witness sees the signatory pressing the keyboard, the witness will not know with certainty what is happening. Thus, it would be possible to ensure that the screen display corresponds to the contents of the information system and that the signatory's keystrokes correspond to his or her intentions only if the information system has been confirmed to effect a trusted path by trusted evaluation criteria.[lx]

However, a secure electronic signature would be able to perform a function similar to the attesting witness by identifying the person purporting to sign the deed. Using a secure electronic signature without a human witness, it could be possible to verify the authenticity of the signature, the identity of the person to whom the signature belongs, the integrity of the document and probably even the date and time of signing. In this sense, a secure electronic signature may even be superior to an ordinary handwritten signature. The advantages of having, besides, an actual witness to attest a secure digital signature would probably be minimal unless the voluntary nature of the signing is in question.[lxi]

Existing legislation worldwide has not gone so far as to entirely replace attestation requirements with electronic signatures, but merely allows the witness to use an electronic signature. The Electronic Transactions Act of New Zealand, for example, provides that the electronic signature of a witness meets the legal requirement for a signature or seal to be witnessed. The technology to be used in making the electronic signature is not specified, but must adequately identify the witness and adequately indicate that the signature or seal has been

witnessed; and be as reliable as is appropriate given the purpose for which, and the circumstances in which, the witness's signature is required.[lxii]

CHALLENGES TO THE VALIDITY AND AUTHENTICATION OF ELECTRONIC SIGNATURES FOR ELECTRONIC CONTRACTS

As stated earlier, the requirements of writing and signatures are generally considered formalities but they also create durable records of the parties in a contract and identify the terms of the agreement.[lxiii] Signatures serve the function of channelling by clarifying the line between intent to act legally and the intent to act otherwise. Parties to a contract are forced to use a particular form and similar agreements must use similar forms. The channelling also affects the decision as to whether a document is legally binding by reducing the need to produce evidence in the case. Thus, channelling is related to evidentiary function.[lxiv]

Affixing a signature is a formality, yet it serves the evidentiary purpose by ensuring the availability of admissible and reliable evidence. These characteristics help in preventing perjury or fraud. Signatures can perform evidentiary functions as follows:[lxv]

a. signature identifies the signer by name;
b. signature identifies a particular characteristic or attribute or status of the signer, rather than the name of the person;
c. signature provides evidence that the signatory has agreed to be bound by the record either by adopting or approving; and
d. Signature provides evidence that the signatory has acknowledged or witnessed or verified the record and not necessarily agreed to be bound by the contents of the document.

The Court of Appeal of New South Wales in Australia was presented with a case to determine the validity of an electronic signature in *Williams Group Pty Ltd v Crocker*[lxvi]. In that case, IDH Modular Pty Ltd opened a credit account with Williams Group and the directors of IDH, including Mr Cocker, appeared to affix their signature electronically to the credit account application, and to a guarantee which was witnessed by IDH's administration manager. The signatures had been inserted using 'Hellofax', an electronic password-protected system that enabled users to sign documents electronically. Mr Crocker had a username and password for

the system but had not changed the password. Williams supplied goods to IDH but IDH went into liquidation without paying and Williams sued Mr Crocker on his guarantee. Mr Crocker successfully defended the proceedings on the basis that although he had been a user of the Hellofax signature, he had not authorised the placing of his signature, and that an unauthorised person must have done so. The Court found that for Mr Crocker to be bound by the electronic signature there would need to be tangible and convincing evidence that he authorised the placement of his electronic signature on the guarantee, or he represented to Williams that a particular person was properly authorised to use his electronic signature.

It has been argued by some jurists that electronic signatures cannot fulfil all of the functions of a traditional signature.[lxvii] It was also perceived that the absence of paper as the principal medium of communication in an electronic environment would lead to a loss of traditional safeguards when the paper was removed as a medium of commercial activities. The Statute of Frauds and the standard business practices require contracts involving the sale of goods to be in writing and signed by the parties. This practice is to ensure that the contents of the contract remain unchanged and forensic experts can detect any alterations made on the paper by looking into the ink marks and handwriting of the parties. It was argued that an electronic contract does not permit such detection, as a computer message may be unsigned and may be tampered without any detection.[lxviii] The increased risk of fraud was perceived as a hurdle.[lxix]

Creating trust in electronic commerce is of great importance for its development. Special rules may be needed to increase certainty and security in its use. However, in the absence of contractual rules, or to the extent that applicable law may limit their enforceability, the legal value of electronic authentication and signature methods used by the parties will be determined by the applicable rules of law, in the form of default or mandatory rules. Such rules may be provided in a variety of legislative texts: international legal instruments (treaties and conventions); transnational model laws; national legislation (often based on model laws); self-regulatory instruments;[lxx] or contractual agreements[lxxi].

Electronic authentication legislation and regulation has taken many different forms at the international and domestic levels.[lxxii] Three main approaches for dealing with the validity and enforcement of electronic contracts and electronic signatures can be identified: (a) the minimalist approach; (b) the technology specific-approach; and (c) the two-tiered or two-pronged approach.[lxxiii]

1. **Minimalist Approach:** Some jurisdictions recognize all technologies for electronic signature, following a policy of technological neutrality. This approach is called minimalist because it gives a minimum legal status to all forms of electronic signature. Under the minimalist approach, electronic signatures are considered to be the functional equivalent of handwritten signatures, provided that the technology employed is intended to serve certain specified functions and besides meets certain technology-neutral reliability requirements.

   The UNCITRAL Model Law on Electronic Commerce provides the most widely used set of legislative criteria for establishing a generic functional equivalence between electronic and handwritten signatures. Article 7, paragraph 1, of the Model Law, provides:

   (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

   (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

   (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

   This provision contemplates the two main functions of handwritten signatures: to identify the signatory and to indicate the signatory's intent concerning the signed information. Any technology that can perform these two functions in electronic form should, according to the Model Law on Electronic Commerce, be regarded as satisfying a legal signature requirement.

   The Model Law is therefore technologically neutral; that is, it does not depend on or presuppose the use of any particular type of technology and could be applied to the communication and storage of all types of information. Technological neutrality is particularly important because of the speed of technological innovation and helps to ensure that legislation remains capable of accommodating future developments and does not become obsolete too quickly. Accordingly, the Model Law carefully avoids any reference to particular technical methods of transmission or storage of information. This general principle has been incorporated into the laws of many developing countries such as India[lxxiv], Mauritius[lxxv] and South Africa[lxxvi]. The principle of technological

neutrality also allows for future technological developments to be accommodated. Furthermore, this approach gives prominence to the freedom of the parties to choose technology that is appropriate to their needs. The onus is then placed on the parties' ability to determine the level of security that is adequate for their communications. This may avoid excessive technological complexity and associated costs.[lxxvii]

2. **Technology-specific approach:** The concern to promote media neutrality raises other important issues. The impossibility of guaranteeing absolute security against fraud and transmission error is not limited to the world of electronic commerce and applies to the world of paper documents as well. When formulating rules for electronic commerce, legislators are often inclined to aim at the highest level of security offered by existing technology. Thus, the legislation is enacted to layout the minimum or required technological standard required for the authentication of electronic signatures.[lxxviii] The practical need for applying stringent security measures to avoid unauthorized access to data, ensure the integrity of communications and protect computer and information systems cannot be questioned.

   In the paper world, business people are in most cases free to choose among a wide range of methods to achieve integrity and authenticity of communications (for example, the different levels of handwritten signature seen in documents of simple contracts and notarized acts). Under a technology-specific approach, regulations would mandate a specific technology to fulfil the legal requirements for the validity of an electronic signature. This is the case, for instance, where the law, aiming at a higher level of security, demands PKI-based applications. Since it prescribes the use of a specific technology, it is also called the "prescriptive" approach.

   The disadvantages of the technology-specific approach are that, in favouring specific types of electronic signature, it risks excluding other possibly superior technologies from entering and competing in the marketplace.[lxxix] Rather than facilitating the growth of electronic commerce and the use of electronic authentication techniques, such an approach may have the opposite effect. Technology-specific legislation risks fixing requirements before a particular technology matures.[lxxx] The legislation may then either prevent later positive developments in the technology or become quickly outdated as a result of later developments. A further point is that not all applications may require a security level comparable with that provided by certain specified techniques, such as

digital signatures. It may also happen that speed and ease of communication or other considerations may be more important for the parties than ensuring the integrity of electronic information through any particular process. Requiring the use of an overly secure means of authentication could result in wasted costs and efforts, which may hinder the diffusion of electronic commerce.

Technology-specific legislation typically favours the use of digital signatures within a PKI. HowPKIs are structured, in turn, varies from country to country according to the level of government intervention.

3. **Two-tiered or two-pronged approach:** In this approach, the legislation sets a low threshold of requirements for electronic authentication methods to receive a certain minimum legal status and assigns greater legal effect to certain electronic authentication methods (referred to variously as secure, advanced or enhanced electronic signatures, or qualified certificates).[lxxxi] At the basic level, legislation adopting a two-tiered system generally grants electronic signatures functional-equivalence status with handwritten signatures, based on technologically neutral criteria. Higher-level signatures, to which certain rebuttable presumptions apply, are necessary to comply with specific requirements that may relate to a particular technology. Legislation of this type usually defines such secure signatures in terms of PKI technology.

   This approach is typically chosen in jurisdictions that consider it important to address certain technological requirements in their legislation but wish, at the same time, to leave room for technological developments. It can provide a balance between flexibility and certainty concerning electronic signatures, by leaving it to the parties to decide, as a commercial judgment, whether the cost and inconvenience of using a more secure method are suitable to their needs. These texts also provide guidance as to the criteria for the recognition of electronic signatures in the context of a certification authority model. It is generally possible to combine the two-tiered approach with any type of certification model (whether self-regulated, voluntary accreditation or a government-led scheme), in much the same way as might be done under the technology-specific approach.

   The first jurisdictions to have passed legislation adopting the two-tiered approach include Singapore[lxxxii] and the European Union.[lxxxiii] They were followed by several others.[lxxxiv] The UNCITRAL Model Law on Electronic Signatures allows an enacting

State to set up a two-tiered system through regulations, even though it does not actively promote it. The UNCITRAL Model Law on Electronic Signatures, in its article 6, paragraph 3, provides that an electronic signature is considered to be reliable if (a) the signature creation data are, within the context in which they are used, linked to the signatory and no other person; (b) they were, at the time of signing, under the control of the signatory and of no other person; (c) any alteration to the electronic signature, made after the time of signing, is detectable; and (d) any alteration made to that information after the time of signing is detectable where the legal requirement for a signature is intended to assure as to the integrity of the information.

Regarding the second tier, it was proposed that countries should not require the use of second-tier signatures for form requirements relating to international commercial transactions and that secure electronic signatures should be limited to areas of the law that do not have a significant impact on international trade (e.g. trusts, family law, real property transactions).[lxxxv] Moreover, it was suggested that two-tiered laws should explicitly give effect to contractual agreements concerning the use and recognition of electronic signatures, to ensure that global contract-based authentication models do not run afoul of national legal requirements.

In Nigerian jurisprudence of evidence, an unsigned document upon which a claim or defence is founded is taken as worthless and inadmissible evidence of such a claim. Even if it is admitted in evidence, the court would not attach any probative value to it. This is because a document, which is not signed, has no origin in terms of its maker.[lxxxvi]

Although some draft bills meant to regulate electronic transactions and contracts in Nigeria are yet to be passed into law, the Evidence Act 2011 recognises the use of electronic or digital signature for the authentication of electronic contracts in contracts where a rule of evidence requires a signature or provides for certain consequences if a document is not signed.

Similarly, the Evidence Act permits that, all electronic signatures 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. While this is a commendable provision, it is however grossly inadequate to deal on all the issues surrounding electronic signatures used for the authentication and validation of electronic transactions.

CONCLUSION

The issues of legality, integrity, confidentiality, non-repudiation and reliability of Nigerian parties in modern Internet and cyberspace transactions and contracts preclude them from using the advantageous technology available to them. This is because there is no way for the parties to demonstrate their desire to be bound within the current legal framework by their transactions. Fortunately, the technology behind electronic signatures is making rapid strides and can overcome many of these concerns. However, the questions about the legitimacy of the parties to the agreement cannot be remedied easily, no matter how sophisticated electronic signatures become. Although electronic signatures are legally valid when one party faces the prospect of finding a way to prove the identity of the original signatories in a situation where another person is not witnessing the signature, the difficulty of using an electronic signature becomes evident. Thus, the onus of resolving the issues and fears lie with Lawmakers and legislators, and governments, who can put electronic signatures on the same level legally as traditional written ones. Once this happens, the fear of reliability will be reduced and transacting parties will become more comfortable with conducting electronic transactions.

Electronic signature technology, as stated in this paper as well as in other works, can affect the future of e-commerce if adequate internationally accepted legislation is implemented. It is necessary for Nigeria to critically address these new legal issues, given the global nature of electronic commerce, and to enact legislation that would facilitate the validity of electronic transactions via electronic signatures. It is evident that electronic commerce will not achieve its potential in Nigeria without the proper legal recognition of electronic signatures and the provision of the legal and institutional infrastructure needed to ensure the protection of electronic transactions. Recognizing that the final solution to electronic signature technology and authentication might not be feasible under international model law, Nigeria, through the National Assembly, must independently establish a legal framework governing electronic transactions and online contracts to ensure that electronic signatures are compatible. This ensures that any legislation that should be enacted should be sure to identify and account for legitimate and enforceable contracts utilizing electronic signatures. The legislation must make it as simple as possible for parties to formalize agreements or contracts as well as enforce same.

REFERENCES

1. Balloon, A. M. "From Wax Seals to Hypertext: Electronic Signatures, Contract Formation and a New Model for Consumer Protection in Internet Transactions" (2001) 50 *Emory Law Journal* 905, 936–7
2. Blythe, S. E. in "Digital Signature Law of the United Nations, European Union, United Kingdom and the United States: Promotion of Growth in E-commerce with Enhanced Security" (2005) 11 *Richmond Journal of Law and Technology* 1
3. Boss, A. H. "Electronic data interchange agreements: private contracting toward a global environment", (1992) 13(1) *Northwestern Journal of International Law and Business* 45.
4. Braley, S. W. "Why Electronic Signatures Can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures", (2001) 7 *Law & Business Review America* 417
5. Carter, W. *Outline of Contract Law in Australia* (Syndey: Butterworths, 1990)
6. Chissick, M. &Kelman, A. *Electronic Commerce: Law and Practice* 3 ed. (London: Sweet & Maxwell, 2002)
7. Davis, C. "Legal Aspects of Digital Signatures" (1995) 11(6) *Computer Law and Practice* 165
8. Davison, A. and M McGregory-Lowndes, M. "Email, Encryption and Electronic Security" (1997) *Law Institute Journal* 26
9. Edwards, L. and Waelde, C. *Law and the Internet: A Framework for Electronic Commerce*. 2nd ed. (Oxford: Hart Publishing, 2000)
10. Fischer, S. F. "Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation," (2001) 7(2) *Journal of Science and Technology Law* 234
11. Forder, J. &Svantesson, D. *Internet and e-commerce law* (Australia: Oxford University Press, 2008)
12. Garrie, D and Borden, R. "Encryption for lawyers", (2016) *Business Lawyer Today* 1.

13. Guadamuz, A. andRens, A. 'Comparative analysis of copyright assignment and licence formalities for open source contributor agreements' (2013) 10 *SCRIPTed* 207

14. Jain, A., Hong, L. and Pankanti, S. "Biometric Identification" (2000) 23 *Communications of the ACM* 91

15. Jones, G. "Failings in the Treatment of Electronic Signatures" (2003) 1 *Hertfordshire Law Journal* 101.

16. Kirchberger, C. *Cyberlaw in Sweden* (Kluwer Law International, 2011)

17. Kisswani, N. M. and Al-Bakri A A 'Regulating the use of electronic signatures given the changing face of contracts' (2010) 7 *Macquarie Journal of Business Law* 53

18. Lillie S 'Will E-SIGN force states to adopt UETA?' (2001-2002) 42 *Jurimetrics* 21.

19. Liu V. et al. "Visually sealed and digitally signed documents", Association of Computing Machinery, ACM International Conference Proceedings Series, vol. 56; and Proceedings of the Twenty-seventh Australasian Conference on Computer Science, vol. 26 (Dunedin, New Zealand, 2004)

20. Low, R. 'From Paper to Electronic: Exploring the Fraud Risks Stemming From the Use of Technology to Automate the Australian Torrens System' (2009) 21 *Bond Law Review* 107.

21. Mason, S. "Electronic signatures in practice", (2006) 6(2) *Journal of High Technology Law* 153.

22. Mason, S. *Electronic Signatures in Law* 4 ed. (Cambridge: Cambridge University Press, 2016)

23. Mason, S. Freedman, C. and Patel, S. "England and Wales" in Stephen Mason (ed) *Electronic Evidence* 3rd ed. (London: LexisNexis, 2012)

24. Maxie, E. 'Digitized Signatures vs. Digital Signatures: A Complete Comparison' 2013 available at http://www.signix.com/blog/bid/99443/Digitized-Signatures-vs-Digital-Signatures-A-Complete-Comparison

25. Mik, E. 'Contracts Governing the Use of Websites' (March 2016) *Singapore Journal of Legal Studies* 70

26. Nelson, S. D. andSimek, J. W. "Encryption made easy: The basics of keeping your data secure" (2016) *Oregon State Bar Bulletin* 2

27. Neville, K. 'The Art and Science of the Email Signature' available at http://www.smashingmagazine.com/2010/02/04/the-art-and-science-of-the-email-signature/ accessed on 17 April 2019

28. O'Gorman L 'Comparing Passwords, Tokens, and Biometrics for User Authentication' (Dec 2003) 91 *Proceedings of the IEEE* 2021.

29. Ølnes, J. and Cook, S. O. Security and signature requirements for e-tendering systems and services (16 August 2016) *Direktoratet for forvaltningogIKT*.

30. Pappas, C. W. 'Comparative US and EU approaches to e-commerce regulation: Jurisdiction, electronic contracts, electronic signatures and taxation' (2002-2003) 31 *Denver Journal of International Law and Policy* 325

31. Rabiyathul B., et al, "Analysis of the Legal Issues of Electronic Contracts", (2017) 116(17) *International Journal of Pure and Applied Mathematics* 147

32. Reed, C. 'Authenticating Electronic Mail Messages—Some Evidential Problems' (1989) 52 *MLR*649

33. Reed, C. 'What is a Signature?' (2000) 3 *Journal of Information Law and Technology* 8 September 2007

34. Schellekens, M. H. M. *Electronic Signatures: Authentication Technology from a legal perspective* (2004) 15

35. Sjoberg, C. M. &Norden, A. "Managing electronic signatures: Current challenges", (2004) 47 *Scandinavian Studies in Law* 79

36. Sjoberg, C. M. 'IT Law for IT Professionals' (2013) *King's College London Slide* 17

37. Sneddon, M. 'Legislation to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact on the Statute Book' (1998) 21(2) *University of New South Wales Law Journal* 334

38. Walden, I. and Savage, N. 'The Legal Problems of Paperless Transactions' (1989) *Journal of Business Law* 102

39. Wang, M. "The Impact of Information Technology Development on the Legal concept – A Particular Examination on the Legal concept of "Signatures" (2007) 15 *International Journal of Law & Information Technology* 253

40. Woods, C. B 'Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions under Electronic Writing and Signature Legislation' (1999) 52 *Oklahoma Law Review* 411

ENDNOTES

[i]Schellekens, M. H. M. *Electronic Signatures: Authentication Technology from a legal perspective* (2004) 15
[ii] Pappas, C. W. 'Comparative US and EU approaches to e-commerce regulation: Jurisdiction, electronic contracts, electronic signatures and taxation' (2002-2003) 31 *Denver Journal of International Law and Policy* 325 at 340
[iii]Schellekens, M. H. M. *op. cit.* p. 16
[iv]Walden, I. and Savage, N. 'The Legal Problems of Paperless Transactions' (1989) *Journal of Business Law* 102, 105.
[v] Edwards, L. and Waelde, C. *Law and the Internet: A Framework for Electronic Commerce* (2nd ed, 2000) 19.
[vi] Cap. I49, Laws of the Federation of Nigeria 2004
[vii]*Lazarus Estates Ltd v Beasley* (1956) 1 All ER 341; *L'Estrange v Graubob* (1934) 2 KB 394
[viii](1844) 5 QB 574; 114 ER 1366
[ix] Ibid. p. 582
[x]Davis, C. 'Legal Aspects of Digital Signatures' (1995) 11(6) *Computer Law and Practice* 165, 165–8
[xi]Reed, C. 'What is a Signature?' (2000) 3 *Journal of Information Law and Technology* 8 September 2007.
[xii]Reed, C. 'Authenticating Electronic Mail Messages—Some Evidential Problems' (1989) 52 *MLR*649;
[xiii]*Omega Bank (Nig.) Plc v. O.B.C. Ltd* (2005) 8 NWLR (Pt.928) 547
[xiv]*Lazarus Estates Ltd v Beasley* (1956) 1 All ER 341
[xv]Sneddon, M. 'Legislation to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact on the Statute Book' (1998) 21(2) *University of New South Wales Law Journal* 334, 339.
[xvi] Reed, C. *op. cit.* (2000) p. 28
[xvii] Alfred E. Weber v. Dante De Cecco 1 N.J. Super. 353, 358
[xviii]*Lobb v. Stanley* (1844), 5 QB 574, 114 E.R. 1366
[xix] [1954] QBD 550 at 56
[xx]*R. v. Moore: ex parte Myers* (1884) 10 V.L.R. 322 at 324
[xxi] The Statute of Frauds was originally passed in Great Britain in 1677 "for the prevention of many fraudulent practices which are commonly endeavoured to be upheld by perjury and subordination of perjury", and has been accepted into Nigeria by the statue of general application.
[xxii] [2003] UKHL 17
[xxiii] [1951] 1 Ch 941 at 947-8 citing approval for the views of Cave J. in *Evans v. Hoare* [1892] 1 QB 593 at 597
[xxiv]*Baker v. Dening* (1838) 8 A. & E. 94
[xxv]*Hill v. Hill* [1947] Ch 231
[xxvi]*Redding, in re* (1850) 14 Jur. 1052, 2 Rob.Ecc. 339
[xxvii]*Cook, In the Estate of (Deceased) Murison v. Cook and Another* [1960] 1 All ER 689
[xxviii]*Brydges v. Dicks* (1891) 7 T.L.R. 215*; Brennan v. Kinjella Pty Ltd.* (1993) NSW LEXIS 7543. Typewriting has also been considered in *Newborne v. Sensolid (Great Britain), Ltd.* [1954] 1 QB 45
[xxix]*France v. Dutton* [1891] 2 QB 208
[xxx]*Goodman v. J. Eban Ltd.* [1954] 1 QB 550; *Lazarus Estates, Ltd. v. Beasley* [1956] 1 QB 702; *London County Council v. Vitamins, Ltd.* [1955] 2 QB 218

[xxxi]Schellekens, M. H. M. *op. cit.* p. 15
[xxxii] Woods, C. B 'Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions Under Electronic Writing and Signature Legislation' (1999) 52 *Oklahoma Law Review* 411
[xxxiii] Blythe, S. E. in 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-commerce with Enhanced Security' (2005) 11 *Richmond Journal of Law and Technology* 1 at 3
[xxxiv]Mason, S. *Electronic Signatures in Law* 4 ed (Cambridge: Cambridge University Press, 2016) p. 199
[xxxv]Kisswani, N. M. & Al-Bakri A A 'Regulating the use of electronic signatures given the changing face of contracts' (2010) 7 *Macquarie Journal of Business Law* 53
[xxxvi] Jones G 'Failings in the Treatment of Electronic Signatures' (2003) 1 *Hertfordshire Law Journal* 101.
[xxxvii] Lillie S 'Will E-SIGN force states to adopt UETA?' (2001-2002) 42 *Jurimetrics* 21.
[xxxviii] Low, R. 'From Paper to Electronic: Exploring the Fraud Risks Stemming From the Use of Technology to Automate the Australian Torrens System' (2009) 21 *Bond Law Review* 107.
[xxxix] O'Gorman L 'Comparing Passwords, Tokens, and Biometrics for User Authentication' (Dec 2003) 91 *Proceedings of the IEEE* 2021.
[xl]Kirchberger, C. *Cyberlaw in Sweden* (Kluwer Law International, 2011) p. 272
[xli]Ølnes, J. & Cook, S. O. Security and signature requirements for e-tendering systems and services (16 August 2016) Direktoratet for forvaltningogIKT at pp. 14 & 36.
[xlii]Sjoberg, C. M. 'IT Law for IT Professionals' (2013) *King's College London Slide* p. 17
[xliii] Wang, M. 'The Impact of Information Technology Development on the Legal concept – A Particular Examination on the Legal concept of "Signatures" ' (2007) 15 *International Journal of Law & Information Technology* 253 at p. 264
[xliv]Mason, S. Freedman, C. and Patel, S."England and Wales" in Stephen Mason (ed.) *Electronic Evidence* 3rd ed. (London: LexisNexis, 2012)p. 360
[xlv]Sjoberg, C. M. &Norden, A. "Managing electronic signatures: Current challenges", (2004) 47 *Scandinavian Studies in Law* 79 at 83.
[xlvi] Ibid. p. 85
[xlvii]Guadamuz, A. &Rens, A. 'Comparative analysis of copyright assignment and licence formalities for open source contributor agreements' (2013) 10 *SCRIPTed* 207 at 216.
[xlviii]Sjoberg, C. M. &Norden, A*op. cit.*
[xlix] Report of the Working Group on Electronic Commerce on the work of its thirty-second session, held in Vienna from 19 to 30 January 1998 (A/CN.9/446, paras. 91
[l]UNCITRAL Model Law on Electronic Signatures, part two, para. 33
[li]Forder, J. &Svantesson, D. *Internet and e-commerce law* (Australia: Oxford University Press, 2008) 50
[lii]Mik, E. 'Contracts Governing the Use of Websites' (March 2016) *Singapore Journal of Legal Studies* 70 at 73
[liii]Chissick, M. &Kelman, A. *Electronic Commerce: Law and Practice* 3 ed. (London: Sweet & Maxwell, 2002)p. 98
[liv] Neville, K. 'The Art and Science of the Email Signature' available at http://www.smashingmagazine.com/2010/02/04/the-art-and-science-of-the-email-signature/ accessed on 17 April 2019
[lv] Emily Maxie 'Digitized Signatures vs. Digital Signatures: A Complete Comparison' 2013 available at http://www.signix.com/blog/bid/99443/Digitized-Signatures-vs-Digital-Signatures-A-Complete-Comparison accessed on 17 April 2019
[lvi] Nelson, S. D. &Simek, J. W. 'Encryption made easy: The basics of keeping your data secure' 2016 *Oregon State Bar Bulletin* at 2
[lvii] Jain, A., Hong, L. and Pankanti, S. "Biometric Identification" (2000) 23 *Communications of the ACM* 91
[lviii]UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 (United Nations publication, Sales No. E.02.V.8), part two, para. 29 (available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html accessed on 6 June 2019
[lix]Garrie D & Borden R 'Encryption for lawyers' 2016 *Business Lawyer Today* 1.
[lx] This is referred to as the "what you see is what you sign" (WYSIWYS) problem in the literature of Liu V. et al. "Visually sealed and digitally signed documents", Association of Computing Machinery, ACM International Conference Proceedings Series, vol. 56; and Proceedings of the Twenty-seventh Australasian Conference on Computer Science, vol. 26 (Dunedin, New Zealand, 2004), p. 287
[lxi] Discussions in Joint Infocomm Development Authority of Singapore and the Attorney-General's Chambers, Joint IDA-AGC Review of Electronic Transactions Act Stage II: Exclusions under Section 4 of the ETA,

consultation paper LRRD No. 2/2004 (Singapore, 2004), parts 5 and 8, available at www.agc.gov.sg, under "Publications" (accessed on 6 July 2019)
[lxii] Section 23, New Zealand, Electronic Transactions Act
[lxiii]Sneddon, M. Ibid. p. 338
[lxiv]Carter, W. *Outline of Contract Law in Australia* (Syndey: Butterworths, 1990) p. 2206
[lxv]Sneddon, M. Ibid. p. 348
[lxvi][2016] NSWCA 265
[lxvii] Davison, A. and M McGregory-Lowndes, M. 'Email, Encryption and Electronic Security' (1997) *Law Institute Journal* 26; Sneddon, M. Ibid. p. 348
[lxviii]Sneddon, M. Ibid.
[lxix] Balloon, A. M. 'From Wax Seals to Hypertext: Electronic Signatures, Contract Formation and a New Model for Consumer Protection in Internet Transactions' (2001) 50 *Emory Law Journal* 905, 936–7
[lxx] For example, Economic Commission for Europe, United Nations Centre for Trade Facilitation and Electronic Business, recommendation No. 32, entitled "E-commerce self-regulatory instruments (codes of conduct)" (ECE/TRADE/277), available at http://www.unece.org/cefact/recommendations/rec_index.htm (accessed on 5 June 2019
[lxxi] for example, Economic Commission for Europe, Working Party on the Facilitation of International Trade Procedures, recommendation No. 26, entitled "The commercial use of interchange agreements for electronic data interchange" (TRADE/WP.4/R.1133/Rev.1); and United Nations Centre for Trade Facilitation and Electronic Business, recommendation No. 31, entitled "Electronic commerce agreement" (ECE/TRADE/257), both available at http://www.unece.org/cefact/recommendations/rec_index.htm (accessed on 5 June 2019)
[lxxii]Boss, A. H. "Electronic data interchange agreements: private contracting toward a global environment", (1992) 13(1)*Northwestern Journal of International Law and Business*45.
[lxxiii]Fischer, S. F. "Saving Rosencrantz and Guildenstern in a virtual world? A comparative look at recent global electronic signature legislation," (2001) 7(2)*Journal of Science and Technology Law* 234
[lxxiv] Information Technology Act, 2000
[lxxv] Electronic Transactions Act 2000
[lxxvi] Electronic Communications and Transactions Act (2002)
[lxxvii]Mason, S. "Electronic signatures in practice", (2006) 6(2)*Journal of High Technology Law* 153.
[lxxviii] Estonia, Digital Signatures Act (2000); Germany, Digital Signature Act, enacted as article 3 of the Information and Communication Services Act of 13 June 1997; Israel, Electronic Signature Law (2001); Japan, Law concerning Electronic Signatures and Certification Services (2001); Lithuania, Law on Electronic Signatures (2000); and Malaysia, Digital Signature Act 1997
[lxxix]Rabiyathul B., et al, "Analysis of the Legal Issues of Electronic Contracts", (2017) 116(17)*International Journal of Pure and Applied Mathematics* 147
[lxxx] Ibid.
[lxxxi]Braley, S. W."Why Electronic Signatures Can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures", (2001) 7 *Law & Business Review America* 417
[lxxxii] Electronic Transactions Act 1998
[lxxxiii] European Union directive on electronic signatures (Official Journal of the European Communities, L 13/12, 19 January 2000)
[lxxxiv] For example, Pakistan, Electronic Transactions Ordinance, 2002 etc.
[lxxxv]UNCITRAL. *Op. cit.* p. 85
[lxxxvi]*Omega Bank (Nig.) Plc vs. O.B.C. Ltd* (2005) 8 NWLR (Pt. 928) 547 at 581 paragraph D, per Tobi JSC.