Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.47, 2016

Electronic Commerce in Nigeria: The Exigency of Combatting Cyber Frauds and Insecurity

Akintunde Abidemi ADEBAYO[1] Alaba Ibironke KEKERE [2]

1. Lecturer, Commercial Law Department, Faculty of Law, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria.
2. Lecturer, Private Law Department, Faculty of Law, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria.

Abstract
Electronic commerce (e-commerce) has grown on such a large scale that there is no commercial activity you cannot embark upon within your home or business premises. This rapid growth in e-commerce has attracted a lot of sellers and buyers alike. There is the evolvement of smart phones, tablets and palm tops which enable the users to buy and pay for things online, do internet banking, pay their bills or to even make a bet anywhere and at any time. These innovations have brought convenience and also contributed to the quality of life of users. The main and distinctive advantage of e-commerce is that it has made life much more convenient for people and also removed various forms of barrier to trade since e-commerce could be conducted through various media. There is also the evolvement of the Automated Teller Machine (ATM), which has largely reduced queues which dominate financial institutions in the past. Now you can deposit or withdraw money without need to physically face a cashier in the banking hall. Despite the benefits and advantages of e-commerce, this technological advancement in the business world is still plagued by some challenges and the major one being security. This paper will therefore, examine electronic commerce, its advantages, the issue of security as a major challenge and concludes with suggestions and recommendations.
Key words: E-commerce, Security, Fraud, Encryption and Password.

1. Introduction

Many economic actors are involved in a modern day e-commerce. They range from large manufacturers to small scale retailers and consumers. This has made it possible for new commercial functions and activities to keep springing up daily.

Geographical barriers have also been removed with the advent of e-commerce therefore; consumers from all over the world now have access to goods and services which prior to the advent of e-commerce were beyond their geographical reach. This in turn, has expanded the existing market and also created new ones.[1] Nigeria for instance, has witnessed several online retail shops springing up in the past ten years. They include; www.konga.com, www.jumia.com, www.olx.com, www.nairaland.com, among others.[2] In other advanced climes such as the United Kingdom, there are, www.ebay.co.uk, www.gumtree.co.uk, among others. Record has it that in Nigeria, persons within the age bracket of 25 and 34 get most of their needs online while persons who are older than 65 are more interested in buying in physical stores than online.[3]

The financial sector has adopted diverse e-payment channels to reflect the global trend in e-payment development. This incidentally has increased the rate of electronic fraud, which has led to the formation of a group known as Nigerian Electronic Fraud Forum which consists of stakeholders in the financial sector in Nigeria.[4]

The insecurity in the cyber space increases even as e-commerce grows.[5] One continually hears on the news of internet banking frauds, online credit card frauds, credit card details of consumers being hacked into, fraudsters illegally using genuine credit card details to purchase goods and services online or even setting up fictitious websites selling products which do not exist in order to get credit card details of consumers.[6] According to Nigeria Interbank Settlement System and the Nigeria Electronic Fraud Forum, about ₦6.2 billion naira was lost to electronic fraud in the financial sector in 2014.[7]

---

[1] H Chan, *et.al, E-Commerce Fundamentals and Application* (New York: John Wiley & Sons Ltd, 2001) p. 7-8.
[2] I Adedapo, "Trends in Online Shopping", *The Nigerian Punch NewsPaper*, 21 December 2015, p.10-11.
[3] *Ibid.*
[4] "Nigeria Electronic Fraud Forum" available online at http://www.cenbank.org/neff/ accessed on 10 December 2015.
[5] K E Oraegbunam Ikenga, "The Nigeria Police and Problems of Cybercrime and Investigation : Need for Adequate Training", (2015) 18 (1) *The Nigerian Law Journal*, 3.
[6] I Adedapo (n.2)
[7] "₦6.2 billion naira lost to electronic fraud in 2014" available online at http://www.punchng.com/business/technology/n6-

Based on all these online cases of fraud and insecurity, there is the need to protect online consumers and also create confidence in them.[1] As a result in increase in online fraud in Nigeria, so many consumers are beginning to have preference for payment at the point of delivery of good (where available) against online payment option.[2] Cyber fraud and criminality in Nigeria has grown to an extent that it has tainted the international image of Nigeria and hindered economic development.[3] Consumers need to be confident that while providing their credit card details online in making payment for goods or transacting business through internet banking and automated teller machine (ATM), that hackers would not have access to their personal details.[4] Bank customers now need to be security conscious more than ever before when carrying out electronic transactions.[5]

In addition to personal security measures, Nigerian banks need to safeguard themselves against electronic fraud. To this end, there is a plan by stakeholders in the financial sector to establish a central risk information centre to take care of banking risks in the country. Also put in place is a central anti-fraud system which is hosted by Nigerian Interbank Settlement System. [6]Until all these security issues are addressed, people and consumers may not be encouraged to participate in e-commerce.

2. Definition of terms

E-commerce has been rudimentarily described as the selling of selling of goods and services over the internet but it is more than that.[7]

E-commerce as Organisation for Economic Cooperation and Development (OECD) points it out entails ‘

> ‘All forms of commercial transactions involving both organisations and individuals that are based upon the electronic processing and transmission of data, including text, sound and visual images. It also refers to the effects that the electronic exchange of commercial information may have on the institution and processes that support and govern commercial activities.’[8]

E-commerce and E-business are often interchangeably used. According to Chaffey, it is not just the buying and selling on the internet but also includes servicing customers and collaborating with business partners.[9] The rapidly changing nature of technology and communications has led to the World Wide Web and E-Commerce being labelled the future of business. The internet has really changed the way businesses and consumers conduct transactions.

Kalakota and Whinston,[10] describe e-commerce as the capability of buying and selling products on the internet and other online services. E-business was described as ‘the transformation of key business process through the use of internet technologies.[11]

In the opinion of Lawal and Ogbu, e-commerce can be categorized into two namely;

a. E-merchandise: selling goods and services electronically and moving items through distribution channels, for example through internet shopping for groceries, tickets, music, cloths, hardware, travel, book, flower or gifts.

b. E-finance: banking, debit cards, smart cards, banking machines, telephone and internet banking, insurance, financial service and mortgages on-line.[12]This aspect of e-commerce has been widely embraced by the Nigerian

---

2bn-lost-to-electronic-fraud-in-2014-onajite/ accessed on 13 December 2015.

[1] I Adedapo (n.2)

[2] I Adedapo (n.2)

[3] K E Oraegbunam Ikenga (n. 5)

[4] B O Jemilohun, “Legislating for Data Protection in Nigeria: Lessons from UK, Canada and India” (2011) 1 (5) *Akungba Law Journal*, 4.

[5] A A Adebayo, “Security and Data Protection Challenges in Electronic Commerce” (Unpublished LL.M Dissertation submitted to Aberdeen Business School, Robert Gordon University, Aberdeen, United Kingdom 2007)

[6] A A Adebayo (n. 12).

[7] “Definition of e-commerce” available online at http://www.primode.com/glossary.html. (accessed on 12 December 2015).

[8] Organisation for Economic Cooperation and Development (OECD) Electronic Commerce: Opportunities and Challenges for Government (The Sacher Report), (Paris, OECD, 1997) at page 11. OECD was established in 1961. It is located in Paris, France. It brings together governments of countries committed to democracy and market economy so as to assist other countries development, contribute to the growth of world trade, maintenance of financial stability, raise standard of living and boost employment.

[9] D Chaffey, *E-Business and E-Commerce Management* (3rd Ed., Harlow: Pearson Education, 2007) pp. 14-15.

[10] R Kalakota and A Whinston, *Electronic Commerce, a Manager’s Guide* (Boston, MA: Addison-Wesley Longman Publishing, 1997) p. 12.

[11] “Definition of e-business” available online at www.ibm.com/e-business (accessed on 10 December 2015).

[12] A Lawal and R C Ogbu, “E-Commerce, Problems and Prospects in Nigeria” (2015) 1 (3) *International Journal of Scientific Engineering and Applied Science,* 230 - 231.

populace. So many Nigerians now make use of electronic and mobile banking as well as payment systems to transfer money from one account to another, obtain bank account statements, pay utility bills such as electricity, water, cable, telecommunication, among others because it offers quicker and more convenient delivery of banking services to customers unlike the physical banking.[1]

3. Advantages of E-commerce.

Modern day technology has made e-commerce possible. The evolvement of e-commerce is one of the best things to have happened to mankind.

Turban et.al opines that consumers and business organisations benefit immensely from e-commerce.[2]

Mark attributes the growth rate of e-commerce to the benefits which people find irresistible.[3]

Some of the benefits of e-commerce include; convenience, speed, variety, bargain, and easy access to more information.

a. **Convenience:** According to Turban et.al.,[4] goods and services could conveniently be bought and paid for online at any time of the day. There are no closing times like we have in physical high street stores. This, saves a lot of time and energy especially for those who have very busy schedule and could not really make out time for shopping on the high street or even those who live in remote areas as all you need to do is place an order online and you get an instant confirmation that you order has been placed. E-commerce according to Chan et.al,[5]therefore promotes trade and businesses by removing time or geographical barriers to trade as you can buy whatever you want to buy only with a click of the mouse.[6]It is now possible for a consumer to order for goods online and to pay in cash upon delivery. This laudable service is available in most of the online retail businesses in Nigeria.

b. **Speed:** Buying goods on the internet is far faster and far more convenient than visiting the physical stores sometimes. It has been observed that e-commerce makes it possible for a higher volume of transactions to be done at a very high speed. Modern day technology has made it possible for orders placed to be directly given to another computer which accounts for all the orders. The computer therefore makes all the necessary shipping arrangements with the suppliers and the consumers in order to ensure goods move out of the warehouses.[7]

c. **Cheap**: It has been observed that, the direct cost of goods bought online is generally cheaper than the prices you find in physical stores.[8]

d. **Variety:** E-commerce avails consumers the opportunity to select from a wide range of products available online. With the use of search engines, consumers can visit the websites of different vendors at any time of the day comparing the prices and buying goods. There is an application called 'price check' which is now available in Nigeria. There are similar applications in other jurisdictions all over the world. The application enables consumers to compares prices of various online sellers before making their choice. [9]

   E-commerce has made it possible for consumers to have unlimited choices and alternatives all over the world. It makes it possible for sellers' production, marketing and distribution costs to be transparent to consumers who can then compare products and of company A to company B and then go ahead to make their choices. This is called 'cost transparency.'[10]

   Consumers always have more to buy online than in any other market. There is diversity in sizes, shapes, colours and styles online which might not exist in physical store as a result of size constraint.[11]

e. **Competition and good bargains:** Another good thing about e-commerce is the ability of online consumers to get good bargains. Warren[12]is of the opinion that e-commerce allows for high competition in a global market. Since there are a lot of vendors and merchants online, there will be competition and

[1] A Lawal and R C Ogbu (n. 19).
[2] E. Turban *et.al, Electronic Commerce, a Managerial Perspective (* 2nd edn., Prentice Hall, 2002) p. 25.
[3] "UPS Lures Dot Coms and Web Integrators to New E-ventures" available online at www.crn.com/it-channel/18814564 accessed on 17 December 2015.
[4] E Turban, *et al*. (n.21) p. 26.
[5] H Chan, *et al*., (n. 1) p. 12.
[6] W Taylor, "Press freedom" (2000) 7, *e-Business Journal*, 71.
[7] A Lawal and R C Ogbu (n. 19) p. 234.
[8] *Taking a smart phone bought from an online store as an example, while the online store sells the smart phone for ₦20, 000. 00 (twenty thousand naira), it may be sold for about ₦22, 000.00 (twenty two thousand naira) or even more in a physical store on the high street.*
[9] A A Adebayo (n. 12).
[10] I Adedapo (n. 2).
[11] I Adedapo (n. 2).
[12] W Taylor (n. 25) p.11.

the market forces of demand and supply force the prices down so online consumers most of the time end up buying goods at prices cheaper than they would have bought in physical stores. Competition in e-commerce therefore has brought about low prices. Some online vendors even go extra miles to offer to ship the goods bought from them free of charge all in order to attract more customers.

f. **Better Information:** A lot of information on a wide range of products could be gathered on the internet. For instance, 'www.pricecheck.com'. The internet is therefore a source of knowledge for people who want the best of all products at the most fair price. Online merchants and vendors could easily update their prices at any time therefore, consumers always have updated knowledge. [1]

Ling, equally identifies the following as the benefits of online bookshop as an aspect of e-commerce.[2] They are: globality; convenience; interaction; personalisation; low rate of returned goods and no pressure of stock.
In a write-up about on online bookshop in Taiwan, the following were identified as benefits of online bookshop in Taiwan.[3] They are: provision of specific services to targeted customers; rich book information; competitive prices; cooperation of publishers, distributors and media writers; deep discount; digitised property ability and launching variable promotions and services periodically.

Other advantages of e-commerce include; inexpensive setting up and management. It is inexpensive, easy to set up and run.

According to Kalakota et.al, e-commerce is good and attractive because it can be used to raise profit while decreasing cost.[4] Since no much human intervention is required in the setting up and running of an e-business, the cost will be far cheaper than physical stores where you will have to employ more members of staff (man power) who will be receiving wages and salaries.

Also in the area of financial services, e-commerce has proven itself to be beneficial and irresistible. Rolf opines that 'the internet has affected virtually all aspects of commerce including the financial sector and has radically changed the banking landscape over the last few years.[5]

From the foregoing, it has been observed that the evolution of e-commerce has brought a lot of opportunities and has also contributed to the development of world economies both in the developed world and the developing world.

4. Security concerns in E-commerce

It has been observed that even with plethora of benefits of e-commerce, the level of insecurity in the cyber space keeps rising on daily basis. Personal credit card details of consumers are not safe; they could be easily hacked into by hackers who are always in promiscuous modes waiting on the internet for victims.[6] So many online consumers are scared to put down their credit card details to buy goods.[7] The security risks and threats could come in various forms. They include: [8] carrying out denial-of-service (DoS) attacks which stops access to authorized users of a website, so that the site is forced to offer a reduced level of service or, in some cases, cease operation completely; accessing sensitive data such as price lists, catalogues and valuable intellectual property, and altering, destroying or copying it; corrupting business information with the use of virus; hacking into financial information about a business and its customers, with a view to perpetrating fraud; altering a business website, thereby damaging the image of the business or directing its customers to another website; satellite transmissions interception; emails are stored on the servers of internet service providers (ISPs) where unauthorized persons could gain access or even internet service providers (ISPs) themselves.[9]

---

[1] "The benefits of e-commerce" available online at http://www.anawebhosting.co.uk/e_commerce.htm, (accessed on 22 January 2016).
[2] H Ling, "Online bookshop in Taiwan" available online at http://cmr.ba.ouhk.edu.hk/cmr/webjournal/u6n4/64_2.pddf (accessed on 28 January 2016).
[3] H Ling (n.33).
[4] R Kalakota (n. 17) p. 54.
[5] B Rolf, "Internet Lures" available at http://news.bbc.co.uk/1/hi/business/651215.stm (accessed on 28 January 2016).
[6] A A Adebayo (n. 12); B O Jemilohun (n. 11).
[7] B O Jemilohun (n. 11).
39. "E-commerce security issues" available online at http://www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1075385862 (accessed on 25 January 2016).
[9] Y Adeniz, "UK government policy on encryption" available online at http://webjcli.ncl.ac.uk/1997/issue1/akdeniz1.html. The ISP instanced being America online (accessed on 29 November 2015).

a. False Escrow: Fraudsters perpetrate fraud by suggesting use of escrow service after winning a bid on items on the online auction sites like eBay. The victim will send the item to the escrow service, never to hear from the scammer or escrow service again. The website of the escrow service will typically go offline after the victim has sent his goods. Some scammers send e-mails masquerading as official e-mails from PayPal to convince the victim that the escrow method is perfectly normal procedure.[1]

b. False online store front scam: This scam is common to online sales sites. A website is set up offering too-good -to- be –real offers on goods, usually electronics such as laptops, cameras, Mp3 players, mobile phones, among others. For undisclosed reasons, payments for such goods cannot be made through traceable means like credit cards, cheques, or money orders. Payments are only made through untraceable means like Western Union, Money gram or e-gold. The buyer will pay and never receive the goods and the buyer will not be able to trace or sue anyone for such payments.[2]

c. PayPal Scam: It is called a 'charge back' or payment reversal fraud, this scam involves online sales businesses and PayPal. It often happens that a locally based scammer will bid for an item on an online auction, and upon winning, the auction will contact the buyer to arrange a time for pick up. The scammer will fabricate an excuse to use PayPal to pay for the item before arriving to pick up the item. The moment the scammer has picked up the item, he will lodge a complaint with PayPal and have the transaction reversed. They do this by either a stolen PayPal account or a fraudulent PayPal account opened with fraudulent credit card. The victim will only receive an email from PayPal telling them the transaction has been reversed.[3]

d. Emails: These emails come in different forms; some of these fraudsters claim to be e-commerce businesses, banks and financial institutions. It is very common for instance to see mails claiming to be from various banks Access Bank Plc, Zenith Bank Plc, Citi Bank, and the rest of them asking for bank details and credit information. Most of the time, they warn that the customer or consumer's account with the bank would be closed down except he or she reconfirms the personal details online. Such details normally include PIN number, expiration date and card number. Some scammers enhance the believability of their offer through the use of a sham website. Such websites can imitate real business websites or a banking websites.[4]

f. Automated Teller Machine: Some fraudsters make use of bank's Automated Teller Machine (ATM) to steal identities and personal details of bank customers. They install equipment on legitimate ATM in at least two places to steal both debit card numbers and also the PIN numbers. The fraudsters will stay in a car very close to the ATM receiving the information transmitted wirelessly from the equipment they have installed on the ATM. This wireless camera is disguised looking like a leaflet holder and it's mounted in a position to view PIN numbers as they are being entered on the ATM. These fraudsters will now use the PIN and card numbers to withdraw money from the bank accounts through the ATM within a very short time.[5]

g. Advance Fee Fraud (419): Also very common lately is the form of appeal for imaginary or well known figures from some African countries that happen to be in some problems and a huge sum of money is promised in return for whatever help rendered. This is called 'Advanced fee Fraud.' As far back as the 17th century, the first case of advance fee fraud was recorded in Europe. It was referred to as "the Spanish Prisoner Fraud" at the time. [6]The scam took the form of a correspondence in which the fraudster would claim to be a prisoner who knew where some buried treasure was located.[7] The "prisoner" would ask for money to bribe the prison guards so that he could escape and get to the treasure. In return for such money, the "prisoner" would promise to share the treasure with the target of the scam.[8] In reality, the "prisoner" was not in jail at all and was simply using the story as a way to get his hands on the target's money. It is otherwise known as 419.[9] It is also called yahoo yahoo. They refer to their targets as Magas or mumu, slang developed from a Yoruba word meaning "fool". Some scammers have accomplices abroad that move in to finish the deal once the initial contact has been made.[10] These scammers devise ways of getting people's personal information and then using them to steal their money. It could either be bank account details, ATM details and personal identification details that are obtained for ATM scams, credit card scams and money transfer scams. The scammers often mention false addresses and use photographs taken from the internet or from magazines to falsely represent themselves. Once the victim's

[1] "The Fake Escrow service Scam" available online at http://scams.flipshark.com/escrowscam.html (accessed on 19 December 2015).
[2] *Ibid.*
[3] B Rolf (n. 36).
[4] A A Adebayo (n. 12); K E Oraegbunam Ikenga (n. 5).
[5] "Fraud Alert" available online at www.met.police.uk/fraudalert/section/atm_fraud.htm (accessed on 30 December 2015).
[6] "What is 419 Scam?", available online at http://whatismyipaddress.com/419-scam (accessed 28 December 2015).
[7] *Ibid.*
[8] *Ibid.*
[9] The name was derived from the section of the Nigerian Criminal Law which deals with obtaining by false pretences.
[10] "Advanced Fee Scam", available online at https://en.wikipedia.org/wiki/Advance-fee_scam (accessed 28 December 2015).

confidence has been earned and money is transferred by the victim, the scammer then introduces a delay or monetary hurdle that prevents the deal from occurring as planned.[1]

All these issues and many more must be addressed and appropriate measures devised. These security measures must be implemented so that they do not inhibit the smooth operation of e-commerce or discourage e-consumers and the intended e-commerce operation.

5. Ways to prevent online fraud and insecurity
Online fraud could be minimised if some precautions are taken. They include:

a. Cautiously dealing in the fraud –prone regions: Some regions are more prone to fraud than others; it is suggested that online merchants and internet users generally be cautious when transacting business making use of their credit or debit card in such regions unless the shopper is otherwise known to the seller. Examples of countries on the list include; Africa- Egypt, Sierra-Leone, South-Africa, Ghana, Nigeria. Asia- Indonesia, Pakistan, Malaysia, Philippines, Singapore, Thailand. Eastern Europe-Belarus, Hungary, Estonia, Latvia, Macedonia, Lithuania, Russia, Romania, Slovakia, Serbia, Yugoslavia and Ukraine.[2]

b. **Free e–mail:** e-businesses and consumers should beware and careful when accepting orders where the return e-mail addresses are undeliverable or from free e-mail services. Consumers can check to see if the address is a free service by putting www. in front of the domain name portion of the address. Buyers with free e-mail addresses are usually fraudulent. They use it so as not to leave any traces of the scam.[3]

c. Mobile phones: Mobile phone numbers are also a warning sign, as they could be anonymous therefore untraceable. Land phones usually are traceable and checkable.[4]

d. Confirmation : In case of any suspicion of fraud, merchants should try to contact the customer to verify some detail of the order, ask them to verify the card number, card security code (last three digits of the number printed on the signature strip), the issuing bank and any other relevant security questions. This may help prove that the card genuinely belongs to the buyer. Merchants should also ensure the billing address, the card holder's name and delivery information all correspond. There might be some elements of fraud in a situation whereby the billing address or the address on the credit card is quite different from the delivery address.[5]

e. Scam e-mails: Consumers should beware of unsolicited e-mails and messages. They should avoid opening such mails. They should get them deleted immediately to avoid the temptation of getting attracted to their too –good –to- be true scam offers.[6] Consumers should also note that fraudulent emails often contain spelling errors and poor grammar.[7]

Consumers should beware of e-mails with a sense of urgency; attempting to rush you into action. Messages like, "Update now or we will close your account...".They are usually fraudulent. Consumers should avoid including their sensitive data as reply to such emails.[8]

Most importantly, online consumers, customers, merchants and other internet users generally should not be greedy and should always avoid shady deals. It has been observed that more than 75% of victims of online fraud

[1] M B Anzaki, "419 Scams and its Impact on the Image of Nigeria" available online at http://thelawyerschronicle.com/419-scams-and-its-impact-on-the-image-of-nigeria/ (accessed on 28 December 2015); A A Adebayo (n. 12).
[2] "Credit card fraud" available online at http://www.floyd.co.uk/mambo/index.php?option=com_content&task=view&id=24&Itemid=59 (accessed 30 December 2015).
[3] *Ibid;* K E Oraegbunam Ikenga (n. 5).
[4] *Ibid.*
[5] A A Adebayo (n. 12).
[6] "Online Fraud Report by National Cyber Security Alliance and bank of America" available online at http://www.infragard.net/library/pdfs/onlinefraudreport_final.pdf accessed 30 December 2015; K E Oraegbunam Ikenga (n. 5).
[7] "Tips for preventing online fraud" available online at http://peoples.rbsnb.com/preventiontips.html (accessed 30 December 2015); K E Oraegbunam Ikenga (n. 5).
[8] *Ibid.*

are greedy individuals who want to get rich quickly. Greedy individuals are more susceptible to being defrauded easily. We must always remember that 'no one would give us anything for free.'

6. Recommendations

All the security worries in the cyber space and e-commerce can be summarized into 3; Confidentiality, Integrity, and Authentication.

a. Confidentiality: ensures a message is kept confidential that only the intended recipient would be able to read it. Encryption should therefore be introduced to provide data confidentiality.

b. Integrity: ensures that the receiver of a message detects in case the content of the message has been altered or tampered with.

c. Authentication: makes sure the identities of the parties involved are verified.[1]

The use of encryption to hide digital content and personal information in e-commerce is essential and highly recommended for online users. It could be in form of trade secrets, confidential references and credit card details. Encryption could be used to determine identity. For instance, a lot of people could be underage therefore not allowed to visit some websites, in such situations, encryption could be used to determine the real identity of the visitors to such sites including their ages.

Encryption therefore is very important to e-commerce. The greater the degree of security required, the greater the cost of encryption.[2] Encryption key governs how plain text is converted or transformed into cipher text. All ciphers rely on keys. Keys are used to encrypt a plain text or to decrypt cipher text. The sender must be able to encrypt the message and the receiver decrypts it. For instance, it could be that one would change a character in his/her name with one or two further in an alphabet to produce a cipher text e.g. Rscwn Xqff. This will not make any sense to anyone who cannot decrypt it.[3]

The initial challenge with encryption is how to communicate securely without having agreed on a key but this has been solved with the development of public key and private (Asymmetric) encryption.[4] Unlike conventional 'symmetric' cryptography, different keys are used for encryption and decryption. For instance, a message encrypted with Jane's public key can only be decrypted using her private key.[5] However, with a public key encryption, it is possible to encrypt a customer's credit card details even in a one–off trade. The seller's public key which is sent out with the order form is used for encryption. The seller is the only one who can decrypt it using his private key.[6]

d. Passwords**:** Passwords are always encrypted for security reasons and not as a plain text. Immediately a user types in his passwords, it should quickly be encrypted and tested against the stored encrypted password. The encryption algorithms should also be stored on the computer.[7]

Access to encrypted passwords should be restricted to privileged users.[8] In such a situation, a hacker therefore will need to have the privileged user's passwords before he could be able to use the encrypted password file to attack the others.

The use of electronic signature in e-commerce is also very helpful when it comes to security of online transactions.[9] E-signature according to e-signature directive [10] in EC is required to verify and permit the authentication of data [11] used while carrying out any transaction on the internet.

E-signature can provide: evidence of identity signatory and integrity of the message; his intention to sign;[12] and his intention to adopt the content of the document as his own.

---

1 V Hassler, *Security Fundamentals for E-Commerce*, (Massachusetts: Norwood Artech House, 2001) p. 5.
2 P Todd, *E-commerce Law*, (Routledge-Cavendish Publishing, 2005) p.106.
3 V Hassler (n. 55) p. 16.
4 V Hassler (n. 55) p. 24.
5 *Ibid.*
6 P Todd (n. 56) p. 112.
7 P Todd (n. 56) p.111.
8 *Ibid.*
9 V Hassler (n.5) p.15.
10 Directive 1999/93/E C of the European Parliament and the Council of 13 December 1999 on a Community Framework for Electronic Signatures.
11 R Barretto *et.al*, "Electronic certification in Brazil and in the European Union" (2005) 2 (1) *e-Signature Law Journal*, 14.
12 N Pope, "Practical considerations in securing electronic signatures" (2006) 2 (2) *e-Signature Law Journal*, 107.

Martin and Pascarelli identified the four categories of e-signature as:[1] the Simple electronic signature;[2] the advanced electronic signature;[3] the Qualified signature;[4] and the Digital signature implemented through asymmetric cryptography.

In the case of Greenwood v Martins Bank Ltd,[5] it was held that e-signature will estop a party from denying his liability for a document which carries his electronic signature. It ensures the signer has done it personally and not delegated it to somebody else.[6]

It gives to the parties involved in contract the desired security and also prevent against future alteration of the document.

7. Conclusion

From the foregoing, it is observed that issue of insecurity is a major challenge when it comes to online transactions in Nigeria. It has far reaching effect on the economy and discourages foreign investment. There is therefore the need to address the earlier identified challenges and put appropriate measures in place in order not to inhibit the smooth operation of e-commerce.

The Nigerian government should collaborate with international agencies on cyber fraud with advanced technologies and equipment so as to curb this menace.

Regular sensitization and orientation particularly targeted at the youths, on the evils of cyber fraud and other related vices should be encouraged and put in place.

Importantly, the Nigerian government should provide gainful employment to the teeming population because when people are gainfully employed and occupied, cyber fraud will be less attractive to them.

Above all, governments should take the issue of cyber fraud seriously by enforcing to the letter the provisions of the Cybercrimes Act 2015 and other related laws. The government should demonstrate its readiness to combat cyber fraud by ensuring that fraudsters and scammers are severely dealt with and punished. This will deter others with similar intentions thereby redeeming the image of the country when it comes to cyber fraud among the comity of nations. As it were, Nigeria is labelled the hub of fraudsters.

Law enforcement agents in Nigeria should be more alive to their responsibilities. They should be trained and re-trained on cyber fraud and how to effectively investigate and prosecute online fraud cases.

Members of the public too have a part to play, they should report suspected cases of online fraud to the appropriate authorities.

The sky will be the limit for e-commerce and the growth of online transactions in Nigeria if only consumers could be assured of the safety of their personal details while transacting on the internet. When there is no security, there will be no trust and lack of trust will result in low patronage and participation in e-commerce as well as other online transactions.

[1] M Luigi and P Roberto, "Electronic signature: value in law and probative effectiveness in the Italian legal system" *(2004) 1 (1) e-signature Law Journal,* pp. 17-22.
[2] Article 2 (1) Directive 1999/93/EC.
[3] *Ibid*., Article 2 (2).
[4] *Ibid*., Article 5 (1).
[5] *(1933) A. C 51*.
[6] Y Akdeniz, et *al*: "Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals", (1997) 2 JILT, available online at http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/ (accessed on 30 December 2015).