Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) DOI: 10.7176/JLPG
Vol.82, 2019

A Comparative Analysis of Civil Liability in Electronic Payment Systems Under the U.S. and Nigerian Laws

Emmanuel Nimbe Olowokere
School of Management Technology, the Federal University of Technology, P.M.B.704, Akure, Nigeria

Abstract
One controversial legal issue in relation to fraud in e-banking is how the losses arising from flaws in electronic payment systems would be distributed between the consumer and financial institution. The paper examines the scope of liability of the consumer and bank for unauthorised Electronic Funds Transfer (EFT) under the U.S. and Nigeria laws. Allocation of liability where a consumer is in the picture is, regulated by legal rules in the U.S. The Central Bank of Nigeria regulates e-payment liability issues through guidelines. The protection accorded the consumer by the U.S. EFT Act is wider and financial institutions share more liability than the consumer as opposed to the situation in Nigeria. Under the Nigerian law, consumers' liability is unlimited. Legal improvements are needed to protect the consumer as the weaker party within the context of electronic payment transfer.
Keywords: liability, risk, consumer, electronic payment system, Electronic funds transfer
DOI: 10.7176/JLPG/82-09

1. Introduction

There is a consensus in literature that information technology has affected various aspects of banking activities,[1] for instance the type of financial services the bank offers its customer[2] to transfer funds electronically within the same borders, or internationally. Electronic payment (E-payment) is a subset of an e-commerce transaction. E-payment systems are the instruments, organizations, operating procedures; information and communication systems employed to initiate and transmit payments from a payer to a payee and for settling payments that is, transfer money[3]. The E-payment channels are the apparatus used to safely and efficiently transfer monetary value in exchange for goods and services as well as financial assets.

Electronic transfer of funds (EFT) is one of the services electronic banking offers in modern time. Today, electronic banking provides consumers with various payment modes such as making payments through public access terminals, for instance Automated Teller Machines; Electronic pay roll systems; direct transfers; Electronic cheques and so on. Consumers enjoy the convenience of EFT technology in the form of ATMs inside and outside banking hours to deposit, withdraw and transfer funds. Money can be transferred faster and the settlement between accounts can be executed almost instantly. There is a cost reduction of funds transfer to the bank and the customer, in comparison to paper-based means such as cheques. Customers can access their accounts and generate payment orders from their offices.[4] There are also many advantages in favour of the financial institutions in the shift to electronic banking and the move towards the so-called 'cashless society'.[5] After the substantial initial capital investment in the technology, financial institutions are finding EFT much less expensive to operate than the traditional labour and paper-based systems.[6] Moreover, financial institutions are now actively scaling down their retail branches, thus heightening their reliance on electronic banking.[7] Whilst the benefits of EFT to both financial financial institutions and consumers are clear, EFT brings with it a number of risks. Problems with the issuance of EFT cards and PINs, evidence of payment, liability for unauthorised transactions, computer malfunctions, security of the system, loss of stop payment ('countermand') rights and errors in accounts are among the central concerns of EFT.

Allocation of liability for losses caused by malpractices in e-banking transactions is agreed to be one of the main legal difficulties affecting customers. That is so in view of the one -sided agreements issued by banks.[8] The legal framework on stakeholders' liability in electronic payment systems is therefore central to building trust and confidence in electronic transactions. Broadly stating, consumer protection law and regulations seek to reduce

[1] Omotubora , A., and Subhajit , B. (2018), " Regulation for E-Payment Systems – Analytical Approaches Beyond Private Ordering", *Journal of African Law*, 62 (2), 281 p. 282.
[2] A Consumer refers to a person or an entity that uses, has used or a potential user of financial products or services of a financial institution, while a Customer refers to a person that has a relationship, by reason of benefitting from financial products or services offered by a financial institution. See S.1.3 of the Central Bank of Nigeria Consumer Protection Framework 2016. The two words are use in this paper interchangeably.
[3] Imafidon, A., (2013), "Challenges of E-banking and Payment Systems in Nigeria" *Journal of the Chartered Institute of Bankers of Nigeria*, p 39.
[4] Mark, H., QC,(2002) Paget's Law of Banking ed, Butterworths, London p. 329.
[5] Federal Bureau of Consumer Affairs (Australia), *A Cashless Society? Electronic Banking and the Consumer* (1995) ch 7.
[6] Procter, L. (1993) "Reforming the Australian Payments System: The State of Play" *The Australian Banker (*3) 135, 135-40.
[7] White, P. (1997) "A Critique of the Self-Regulation of Electronic Funds Transfer in Australia" (M Bus Minor Thesis, Victoria University of of Technology 9.
[8] See White, P., and Islam, S. (2008), "Formulation of Appropriate Laws: A New Integrated Multidisciplinary Approach and an Application to Electronic Funds Transfer Regulation, Berlin: Springer-Verlag Berlin Hedelberg. p. 28.

uncertainties for both consumers and financial institutions regarding liabilities related to electronic payments, to provide protection against unauthorized or erroneous electronic transactions that access consumer accounts by setting guidelines to allocate liability for unauthorized transactions as well as imposing documentation and record-keeping requirements to assist consumers in detecting and remedying disputed transactions.[1]

A number of countries have enacted legislation on electronic commerce for the aim of protecting consumers. However, studies indicate that these pieces of legislation do not adequately protect consumers using electronic payment system as they do not address the important aspect of how to fairly allocate losses between a consumer and a financial institution.[2] A similar observation is made in respect of e-commerce legislation in the APEC region.[3] Nigeria operates electronic banking without any specific legislation in this area or on e-payment, unlike the USA (U.S.) which has specific legislation to regulate EFT which contains liability regime for unauthourised electronic payment transactions. The paper examines the extent the consumers are protected from third party fraud, faults on the part of financial institutions, and consumers' own carelessness. The paper gives an overview of consumer e-payment systems, followed by a review of threats to consumer e-payment systems. The remaining parts of the paper cover documentation of EFT, legal and regulatory frameworks for allocation of liability for financial loss arising from EFT under the U.S. and Nigerian laws.

2. Consumer Electronic Payment Systems

The terms 'Electronic Payment Systems' and 'electronic banking' are identified with any machinery facilitating an electronic payment in monetary value. Electronic funds transfer[4] is another term used to refer to the action of using electronic technology. Electronic Funds transfer has been described as the third of the great ages of payment, the first being payment by cash (notes and coins) and the second being paper based payment (for instance, cheques).[5] Kethi Kilonzo takes "electronic funds transfer" or "electronic banking" to mean "any transfer of funds initiated or processed using electronic techniques."[6] EFT means the movement of an amount of money from a customer's bank account to another's bank account by electronic means.[7] In section 903(6) of the U.S Electronic Funds Transfer Act,[8] the term "electronic fund transfer" is broadly defined as any transfer of funds, other than one originated by check, draft, or similar paper instrument, which is initiated electronically and authorizes a financial institution to debit or credit a consumer's asset account. To prevent confusion, the law specifically enumerates several well-known forms of electronic fund transfer that it intends to include within the definition: electronic point of- sale transfers, automated teller machine transactions, deposits or withdrawals of funds through the ACH mechanism, and transfers initiated by telephone.[9] At the same time, it clearly emphasizes that the general definition is not necessarily limited to those particular types of EFT services.[10] The expansive legal definition stated above is designed to encompass future EFT innovations that will undoubtedly evolve after the passage of the Act. The Indian Payment and Settlement Systems Act defines electronic funds transfer as "any transfer of funds which is initiated by a person by way of instruction, authorization or order to a bank to debit or credit an account maintained with that bank through electronic means and includes point of sale transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfers initiated by telephone, internet and card payment".[11] An electronic funds transfer is simply an instruction given by a customer to his bank for transfer of an amount of money to the payee. The significant difference between paper-based fund transfer and EFT is the way the payment instruction is created. EFT transactions are initiated by a payment instruction from the customer to his bank to transfer, or collect, money from one bank account to another by electronic devices.[12] An ETF is commonly initiated by means of an "access device" issued to the consumer by the financial institution, which is capable of accessing the account from which the customer is permitted to withdraw. An access device is defined as a card, code or other means of access to a consumer's account or any combination that may be used by the consumer for the purpose of initiating electronic funds transfers. The term includes debit cards, personal identification numbers, but does not include

[1] White, P., and Islam, S., ibid p.3
[2] See McCarthy, J., (2002) "Consumer Protection in Contemporary Electronic Payment Systems:- A Familiar Wolf in Digital Clothing?" *C.O.L.R.* II, www.ucclawsociety.com/colr/editions/2002/2002- 2.pdf, accessed on 28 December, 2018.
[3] See Report of the Electronic Commerce Steering Group, "Approaches to Consumer Protection within APEC Region" October 2002, www.nacpec.org/docs/Approaches_to_consumer_protection.pdf. accessed on 28 December, 2018.
[4] EFT is a technology (one of the electronic commerce technologies) that allows the transfer of funds from the bank account of the one person or organization to that another.
[5] Kethi, D. (2007) "An Analysis of the Legal Challenges posed by Electronic Banking", *Kenya Law Review* (1) 323.
[6] Ibid.
[7] Arora, A., (1988), Electronic Banking and the Law, IBC Publishing p. 7.
[8] 15 U.S.C. § 1693a (6) (Supp. 1978).
[9] Ibid
[10] Ibid.
[11] Section 2 (c) Payment and Settlement Systems Act, 2007.
[12] Ellinger, E., *et al.,* (2011), Modern Banking Law p. 562; Sappideen, R., (2003) "Cross-border Electronic Funds Transfers through Large Value Transfer System, and the Persistence of Risk", *Journal of Business Law* 13 584 p. 585.

magnetic tape or other devices used internally by financial institutions to initiate the electronic funds transfer.[1]

Electronic payment systems exist in a variety of forms, which can be divided into two groups: consumer activated systems and non-consumer activated systems[2]. Non consumer-activated or wholesale payment systems exist for non-consumer transactions. In non-consumer activated systems it is the bank which normally selects and activates the system. Some corporate or institutional customers may be given direct access to these systems, but the bank's personal account holders do not have similar direct access. They include transactions initiated among and between banks, corporations, governments, and other service firms.[3] Consumer activated or retail electronic systems encompass transactions involving personal account holders as opposed to corporate account holders. In consumer activated electronic funds transfer systems, cards and Personal Identification Numbers[4] facilitate access to funds. Sound banking practice requires that no account be debited unless the authenticity of the paying bank customer's instructions can be established to the satisfaction of the bank where the paying customer's account is maintained. This is because a successful challenge by the customer when debiting their account requires the account holding institution to reverse the debit. A successful challenge may further expose the account holding institution to liability for consequential loss, which may be substantial where a wrongful debit left the account with insufficient funds to meet valid payment instructions, which were consequently dishonoured. To this end, the confidential personal identification number is designed to serve as an electronic signature.[5] Over and above the signature serving as a means of verification and identification of the payment message, it doubles up as the customer's mandate to the bank to pay. The card user is under an obligation to ensure that his access device is kept secure and his personal identification number secret. This duty is often expressly provided for in the agreement between the consumer and bank.

3. Threats to Consumer Payment Systems

3.1 Data Breaches

Security challenges arise on account of unauthorised access to a bank's critical information stores like accounting system. Data breaches occur primarily when outsiders gain unauthorized access to digitized information. Customers have to provide credit card and payment account details and other personal information online. These data are sometimes transmitted in an unsecured way. Providing these details by mail or over the telephone entails security risks.[6] The majority data breaches are committed by outsiders, although insiders account for a significant share.[7] Most incidents are a result of stolen laptops or desktop computer, followed by exposure of information on the Internet or email and hacking.[8] Misuse of data is more likely if it is identity-level information, such as social security numbers, and obtained through deliberate hacks or stolen computer hardware. The resources available to hackers also determine the potential for fraudulent use of stolen data.

A breach of security could result in direct financial loss to the bank. Thus, access control is of paramount importance. Controlling access to banks' system has become more complex in the internet environment which is a public domain and attempts at unauthorised access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, or disgruntled employees. Employees could surreptitiously acquire authentication data in order to access customer accounts, or steal stored value cards. Inadvertent errors by employees may also compromise a bank's systems. Breach of data security could lead to frauds and unauthorised transactions.

3.2 Risks Associated with Electronic Payment Instruments

Specific risks associated with the consumer payment mechanisms which could result in harm to the consumer have been identified.[9] Credit and EFT debit cards generally have no value in and of themselves.[10] Consumers can usually get replacement credit cards and EFT debit cards quickly, under the rules that apply to each particular

[1] Kethi, D. op cit. p. 333.
[2] Mark, H. Pagets Law of Banking, op cit p. 264.
[3] Ibid, p. 265.
[4] Personal Identification Number is a relatively inexpensive means of customer identification in the form of a secret code intended for the sole use of the cardholder and designed to authenticate the cardholder's instructions given at a terminal.
[5] Vincenzo, S. "Digital Signature Legislation in Europe: Virtual Banking and Electronic Payment", Sept International Bar Association 2000 conference, The Netherlands, p12. Prior to the amendment of the Nigeria's Evidence Act (2011), there was no clear statement as to the admissibility of electronic evidence via forensic analysis but its amendment in 2011 brought succour to disputes resolution involving e-transactions. See for example, section 84 of the Evidence Act, 2011.
[6] Hariom, T. , and Abhishek, S. (2016) "The Study of Electronic Payment Systems", *International Journal of Advanced Research in Computer Science and Software Engineering* 6 (7) 297 p. 298.
[7] Richard, J. (2010) The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy Workshop on the Economics of Information Security Harvard University p. 4.
[8] Ibid.
[9] Board of Governors of the Federal Reserve System of the USA, *Report to Congress on the Application of the Electronic Funds Transfer Act to Electronic Stored-Value Products* (1997) 2. White, P. op cit.
[10] Ibid 30.

card's system. Financial institutions provide this service to make their products more attractive. Consumers may lose the entire balance on an EFT card and PIN if they are lost, stolen, or damaged. Consumers also face the risk of financial loss due to unauthorised use of a payment instrument, which may or may not result from the instrument being lost or stolen.[1] Unauthorised use is a relatively common problem for several types of payment instruments, such as cheques, EFT debit cards and credit cards.[2] With EFT cards, often an unauthorised user needs only the information from the card and not the card itself. Thus, consumers who are particularly concerned about theft or unauthorised use may choose to use payment instruments with refund capabilities, and they may be willing to pay for this extra degree of security in cases involving larger amounts of funds.

If an error occurs in the processing of a payment, the payment may be made to the wrong party or for the wrong amount.[3] Malfunctions also could occur in the use of EFT cards. Such disruptions or malfunctions could cause a temporary inability to complete a payment or could cause financial losses.[4] Consumers may face the risk that a particular payment instrument will be dishonoured by the issuer or drawee. Payment instruments may also be returned because of the default of the issuer or drawee. It should also be stated that for various reasons, a consumer might be unable to use a particular payment mechanism.[5] This situation would not necessarily result in a financial loss to the consumer but might unexpectedly prevent a consumer from discharging a debt or obtaining goods or services, result in late fees or other penalties, or at the very least, cause embarrassment.[6] A consumer might be unable to use a payment instrument because of a defect in the instrument. For example, a credit card or EFT debit card might have a demagnetized strip or a damaged chip, causing the card to be rejected by a card-reading machine. To encourage the use of their products, banks and other financial institutions generally provide replacements for damaged cards relatively quickly. Consumers typically reduce risks that they will be unable to make payments by carrying more than one form of payment with them. In doing so, they must weigh the benefits of maintaining access to additional payment options against any inconvenience and fees involved in doing so.

Misuse of products and services by customers is another source of risk. The risk increases due to inadequate education of customers by banks, on security measures during the verification of electronic money transfers. Personal information of bank customers who participate in electronic banking (credit card number, bank account number, etc.) must be specially protected during the electronic money transactions. Misuse of payment instrument may lead to the risk of identity theft. This occurs when the attacker have little information about the victim, and will use this information to perform illegal transaction on the victim's account acting like the legal owner of the account. This attack normally occurs when attacker has gotten information like password, PIN number and so on. Identity theft can be avoided by strongly guiding financial information such as password and PIN.[7] There are incidents of the ATM cardholders being forced by thieves to withdraw funds from their accounts through a public access terminal. The Nigeria ATM cardholder unlike his United States counterpart is made to be liable for his account debited by the amount of withdrawals at such circumstances.

3.3 E-Payment Fraud

The problem of fraud is common to all payments systems and dates back to ancient times. "The fertility of man's invention in devising new schemes of fraud is so great, that the courts have always declined to define it … reserving to themselves the liberty to deal with it under whatever form it may present itself." Graycar and Smith define fraud as an "act or instance of deception, an artifice by which the right or interest of another is injured, a dishonest trick or stratagem."[8] Today, the use of technology has brought about the idea of e-fraud. Bergmen[9] define e-fraud as "a deception deliberately practiced to secure unfair or unlawful gain where some part of the communication between the victim and the fraudster is via a computer network and/or some action of the victim and/or the fraudster is performed on the computer network." Graham[10] defines e-fraud as "a fraudulent behaviour connected with computerization by which someone intends to gain dishonest advantage". In this definition e-fraud equates to, and supersedes, the term computer fraud. The US Department of Justice (DOJ) defines e-fraud as "a fraud scheme that uses one or more components of the Internet – such as chat rooms, e-mails, message boards, or web sites – to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the

[1] Ibid 31-2.
[2] Ibid 31.
[3] Ibid 32.
[4] Ibid 33.
[5] Ibid 35-6.
[6] Ibid 35.
[7] Ekwueme, C., Egbunike, P., and Amara O. (2012), "An Empirical Assessment of the Operational Efficiency of Electronic Banking: Evidence of Nigerian Banks" *Review of Public Administration and Management 1(2)* 377.
[8] Graycar, A and Smith, R. (2002), "Identifying and Responding to Electronic Fraud Risks", Australian Institute of Criminology, http://www.aic.gov.au/media_library/conferences/other/graycar_adam/2002-11-registrars.pdf accessed December 15, 2018.
[9] Bergman, B. (2005), "E-fraud – State of art and countermeasures" http://www.ep.liu.se/exjobb/ida/2005/dd-d/029/ accessed December 15, 2018.
[10] Graham, T. (2002), "Dispute resolution: E-Fraud and Jurisdiction", http://www.tjguk.com/topical/litigation/efraud_and_jurisdiction_winter2001.html accessed December 15, 2018.

proceeds of fraud to financial institution or to other connected with the scheme". The definition given by the US Department of Justice is consumer oriented.

E-payment frauds have a multiplicity of types and there is no exact number or fixed list of these types. Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorised funds from an account. Cardholders can mitigate this fraud risk by checking their account frequently to ensure constant awareness in case there are any suspicious, unknown transactions or activities. When a credit card is lost or stolen, it may be used for illegal purchases until the holder notifies the issuing bank and the bank puts a block on the account. Cloning is another e-fraud and it refers to the manufacture of counterfeit cash cards. Data on the magnetic stripe of cash card is acquired through devices informally called "skimmers". They are loaned out to individuals employed in retail stations like restaurants and garages, who have the opportunity to double swipe a customer's card. The skimmer is returned to the card cloning factory where they use the data collected to make counterfeit card, the original owner of the card is thereby defrauded. When the subsequently made card is sold, unsuspected buyers are defrauded. When the clones are used to purchase goods and services (online), the sellers are defrauded.[1] This means of counterfeiting cash card by using magnetic devices is also employed by fraudster and they normally place the device at ATM stations or POS machines installed in supermarkets. The device captures the information entered by a card holder and then the fraudster detaches the device and then goes to a cloning factory to produce a replica of the original card using the information captured.

In site cloning the fraudster clones an entire site or just the payment page of the site where the customer makes a payment. The customer feels that he is viewing the real site. The customer handovers a credit card detail to the fraudster and then fraudster sends the customer a transaction receipt via e-mail as real site. Thus the fraudster has all detail of the customer credit card so he can commit fraud without customer's awareness.[2]

One of the most common identity theft techniques in Nigeria is social engineering. The social engineering attacks aim at either coercing or tricking an individual into disclosing his personal information such as bank account details, emails details and so on. Under social engineering, the three prevailing identity theft techniques are e-mail based phishing scam, Short Message Service (SMS) scam and phone calls related scam.[3] Online banking fraudsters also have new tools in their possession that is suitable to use with any advance crime ware. There are programs such as "sniffers" which can be set up at web servers or other critical locations to collect data like account numbers, passwords, account and credit card numbers. It causes customers to unwillingly download Malware, a computer code download with bad intention to harm customer by collecting customers' information.[4] They also have a new form of attack spyware such as Trojan horses and kelloggers. Another common method that is used to disrupt the security of the e-payment system is a denial-of-service (DoS) attack or a distributed denial-of-service attack (DDoS) that involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target. By doing this, they disrupt electronic communications[5].They attempt to make computer resources unavailable to its intended users. The DoS attacks typically target sites or services hosted on web servers such as banks or credit card payment gateways. The illegitimate use involves the use of information by unauthorized persons or for unauthorised purposes. It is to be noted that the aforementioned activities are crimes in most countries like the U.S. by virtue of the provisions of Electronic Communications Privacy Act 1988 and Computer Fraud and Abuse Act 1991.[6] In Nigeria, some of these activities constitute crime by virtue of some specific legislation.[7]

Fraud reduces the efficiency of the payment system because it degrades operational performance and increases costs—not only for the parties whose payments are compromised but also for everyone participating in the system. When executed successfully, payment fraud can lead to adverse consequences for participants at different points along the transaction processing chain. For instance, when a criminal steals a payment card and uses it (or its information) to purchase an item, the legitimate cardholder's liability for the fraudulent transaction is limited by statute or regulation. However, participants further down the payment chain—such as the card-issuing bank or a merchant—are often likely to incur losses for such fraudulent transactions.[8]

[1] Ibid. p. 44.
[2] Akshada, K., Chhajed, K,. and Kapse, A. (2017) Review on Fraud Detection in Electronic Payment Gateway, *International Research Journal of Engineering and Technology (IRJET)* 04 (01) p. 841
[3] Joseph, C., and Geraldine, E. (2017), "Internet Banking: Identity Theft and Solutions - The Nigerian Perspective *Journal of Internet Banking and Commerce,* 22, (2) , 1 p. 4
[4] Rashad, Y., and Abu Bakar, S.(2011), "Electronic Banking Fraud: The Need to Enhance Security and Customer Trust in Online Banking", *International Journal in Advances in Information Sciences and Service Sciences* ,310 (61)505 pp. 505-506.
[5] Niranjanamurthy, M., and Dharmendra, C. (2013) "The study of E-Commerce Security Issues and Solutions", *International Journal of Advanced Research in Computer and Communication Engineering* 2 (7).
[6] In Britain, they are crimes by virtue of the provisions of the Computer Misuse Act 1990.
[7] section 6 (b) of the Economic and Financial Crimes Commission Act, 2004. See also Cybercrime Act 2015.
[8] The actual allocation of losses will depend on the circumstances of the transaction and payment card network rules.

3.4 Failure to Effect Transfer of Funds

A bank as a general rule is under a duty to act in accordance with its customers' mandate and to carry out its services with reasonable care and skill. In the event a bank fails to act correctly on a payment order received from its customer, then the bank may be liable for breach of duty.[1] However, the operation of electronic payment system entails the possibility of human errors and malfunctions during execution of instructions. Human error may be caused by either a customer or the bank electronic payment system in the course of processing a payment.[2] Accidentally, a wrong person may be paid, e.g., because a wrong account number has been keyed in or because a wrong account number has been given.[3] This has the effect that, if the payer keys in the wrong account number the payment will be made to the holder of the account number that has been keyed in. The mistake may only come to light when the intended recipient tells the payer that the payment has not been received. When the payer tries to find out where the payment has actually gone, he may be told that the recipient's name cannot be released for reasons of confidentiality. Their bank may claim that it acted on the basis of the instructions it was given, that is, the account number. The recipient's bank may claim that it has no liability because it acted on the instructions it received from the payer's bank. An error may be caused by the negligence of a customer in not keeping his card safely and the same may be used by a third party to draw money. In this case, the machine, for example an ATM, cannot detect that a certain card belonging to someone has been used by someone else. This is why the House of Lords, quoting a witness, said "computers are fast, reliable and stupid. Human beings are slow, unreliable and intelligent."[4] Errors in the electronic payment systems may be caused by the failure of a transaction to be completed (e.g., a deposit at an ATM is not credited to the consumer's account or a payment to a third party is not made). Second, an e-banking transaction may be executed for an incorrect amount. Third, payments may be made to a wrong party or at a wrong time.

Malfunctions could occur in the use of e-banking channels, consequently causing disruption that may lead to temporary inability to have payment completed or could cause financial losses.[5] Ordinarily, banks may assert that the malfunctions are not due to negligence on their part, but due to the operation of the system, particularly when outdated or cheap technologies are used, in which case it is arguable that the banks should be liable for losses incurred by the customer.[6] It has been a common practice for terms and conditions prepared by a number of financial institutions to disclaim liability for failure to carry out a transaction in the event of mechanical failure of equipment or transmission problems, or unavailability of services or where circumstances beyond the bank's control prevent the transaction from being effected.[7]

From the above, the following occurrences may lead to unauthorized transfers:[8]

i. Cards may be stolen or otherwise reach unauthorized hands.
ii. Card information may be obtained by the physical examination of the card or a record of a legitimate card transaction.
iii. Card information may be intercepted in transit, particularly over phone lines or the Internet.
iv. A PIN, any other secret code or password, as well as a private key needed for a digital signature, may be improperly recorded or kept by a customer so as to facilitate breach of confidentiality and availability to unauthorized persons.
v. Short PINs and other codes may be correctly guessed. Similarly, secondary security information, facilitating access to phone banking, such as mother's maiden name or wedding anniversary, may be known to a relative or unfaithful friend who may become an unauthorized user.
vi. The confidentiality of a PIN or any other secret code or password shared between the customer and the financial institution may be breached by insiders with the financial institution.
vii. Security information may be intercepted in telephone banking (where available) and to a lesser degree in Pc as well as Internet banking.[9]

[1] *Ibid.*
[2] Islam and White P. *op.cit.,* p. 22.
[3] See Tyree, A. "Mistaken Internet Payments", ttp://austlii.edu.au/~alan/mistakenepayments, html, accessed December 15, 2018.
[4] See *Agricultural, Horticultural and Forestry Industry Training Bord v Kent Same Tawell & Sons (a firm)* [1970] All ER at 304. The case is relevant as it shows that computers are not always such perfect – errors are likely to occur depending on what was fed on them by human beings.
[5] Ibid., p. 26.
[6] The decision of the House of Lords in *General Clearing v Christmas* [1953] A.C. 180 draws an inference that banks are expected to make use of the latest technology.
[7] Reed, C.(1994) "Consumer E-banking", 11 JIBL 451 p. 462.
[8] For a thorough discussion, in connection with electronic consumer systems and the authentication of consumer payment instructions, see Bohm, B., and Gladman, (2000), "Electronic Commerce: Who Carries the Risk of Fraud?" *The Journal of Information, Law and Technology*, 3 http://elj.warwick.ac.ukjilt/00-3/bohm.html accessed: January 17, 2019.
[9] In general, intercepting the content of traffic between modems is much more difficult than with voice calls. At the same time, if the consumer gains access through a local network such as that of his or her employer, additional interception risks may be involved, where the employer's local network operates a firewall to protect its internal computer system from external attacks, which may prevent security protocols from "end to end" between the financial institution's system and the PC on the customer's desk.

viii. Unless a customer and a financial institution exchange messages signing respective private keys and verified by means of their public keys, that is, unless they exchange messages digitally signed, the customer's communication over the Internet may be diverted to a fraudulent imitation system so as to reveal to the owner of the fraudulent site transaction and security information.[1]
ix. To some extent, the security of banking computer systems has not been fully established. Regardless, serious concerns exist with respect to customer Pc software security. Security may be breached in the course of software installation by a dishonest "expert" neighbour or friend. PCs used on the Internet are vulnerable to attacks in which software is remotely installed to capture and transmit the user's keyboard data to a remote location. An even more potent attack would be based on a computer virus. Such attacks may capture security and account information. Even a private key may be compromised.
x. Secret data held in hardware - for example, in smart cards - are much less vulnerable to being discovered by an attacker. However, hardware solutions are not infallible; many smart cards are vulnerable to a fake machine extracting their secrets by observing the power they consume while calculating a digital signature. As well, solutions bypassing PCs require the card to have a powerful processing capability of its own which raises considerable cost implications. A required PIN may be entered into a small keypad and a digital signature may be processed in the card. Nevertheless, it is only the use of biometric data that could secure safe communication of security information.[2]

4. Documentation of Electronic Funds Transfer

In determining liability for losses in electronic transactions, where disputes occur must be examined with log files that contain the details of such transaction. The log files provide easy means to detailed information as to the IP address of the computer used, where the transaction took place (location), username and password used to transact the service. It can be used in forensic investigation and identification of culprits.

The documentation requirements for EFT are contained in the U. S. EFT Act. Except where technological limitations preclude concurrent documentation such as in "pay-by-phone" bill-paying systems, the Act requires that relatively complete paper documentation of every electronic transaction be made available to the consumer at the time of the transaction.[3] A receipt is required for each electronic fund transfer initiated by a consumer at an electronic terminal, including POS terminals, ATMs, and cash dispensing machines, but not ordinary telephones.[4] The Act states that, at a minimum, the terminal receipt must set forth the type of transfer, the amount involved, the date initiated, the account involved, the identity of any third party involved, and the location or identification of the terminal.[5] Financial institutions may provide receipts only to consumers who request one.[6]

Section 906(c) of the Act[7] mandates a periodic statement for each account of a consumer that may be accessed by means of an electronic fund transfer. The periodic statement must be provided for each month in which an electronic fund transfer affecting the account has occurred, and, in any event, at least every three months. The periodic statement must contain four basic elements. First, it must set forth the same information required for electronic terminal receipts. Second, the periodic statement must show the total amount of any fees or charges for electronic fund transfers or account maintenance during the relevant cycle. Third, the statement must contain the beginning and closing balances in the consumer's account. Lastly, it must provide the consumer with the address and telephone number to be used for making inquiries or providing notice of errors contained in the periodic statement. There are two specific exceptions to the monthly periodic statement requirement. First, if the account is a passbook account that may not be accessed by EFT other than preauthorized credits to the account, financial institutions may, in lieu of a periodic statement, update the passbook to reflect intervening electronic transactions each time it is presented by the consumer. Second, if the account is a non-passbook account that may not be accessed by EFT other than preauthorized credits to the account, the financial institution may provide a periodic statement on a quarterly basis, rather than each month in which a transfer occurs.

In Nigeria, some of the Central Bank of Nigeria (CBN) regulations cater for e-payment documentation. Regulation on Instant Electronic Funds Transfer provides that customers are required to be provided with Funds Transfer receipt as transaction evidence.[8] A terminal receipt is therefore required at any time an electronic transfer

[1] In Pc banking, the customer dials the telephone number of the financial institution's system, and it would be very difficult for an outsider to divert the call to an imitation system. Conversely, the Internet has a much more complex system of addresses than the telephone network, and is much more vulnerable to diversion.
[2] Geva, Benjamin. (2003) "Consumer Liability in Unauthorized Electronic Funds Transfers" *Canadian Business Law Journal* 38 (2) 207 pp. 226-227.
[3] *See, e.g.,* EFT Act, § 906, 15 U.S.C. § 1693d (Supp. 1978).
[4] Ibd, § 1693a(7) (Supp. 1978).
[5] Ibid, § 906(a), 15 U.S.C. § 1693d(a) (Supp. 1978).
[6] Regulation E (Staff Commentary 205.9(a)-1).
[7] 15 U.S.C. § 1693d(c) (Supp. 1978).
[8] Section 5.2 (13) Regulation on Instant Electronic Funds Transfer 2018. This Regulation covers Instant Electronic Funds Transfer Services in Nigeria on various payment channels and any payment platform that seeks to provide Instant Electronic Funds Transfer Services.

is initiated by a consumer at a public access terminal. The terminal receipt clearly certifies the amount of the transfer, the calendar date the consumer initiated the transfer, the time and the balance in the consumer's account. It is a breach of the bank's obligations to its customers not to produce the above receipt. Section 1.3 (4) requires that the ATMs should issue receipts, where requested by a customer, for all transactions, except for balance enquiry, stating at a minimum, the amount withdrawn, the terminal identity, date and time of the transaction.[1] Further, issue of receipts is immediately followed by bank alerts through a platform chosen by the consumer, containing statements evidencing the electronic funds transfer at terminal or any other transaction. In such a case any unauthorized transfer, either through the inadvertence of the bank or its customer, will be detected and any necessary investigations and corrective measures put in place. It is also the bank's duty to issue regular bank statements so as to enable a consumer to verify any unauthorised electronic funds transfer. Consumers are required to be provided with the statement of financial position at all times.[2] The consumer on the other hand has a duty to promptly verify its correctness. In addition, section 1.1 (5) of the Guidelines on Automated Teller Machine (ATM) Operations requires all ATM systems to have audit trail and logs capabilities, comprehensive enough to facilitate investigations, reconciliation and dispute resolution.[3] Also, the CBN acknowledges that Mobile phones are increasingly being used for financial services in Nigeria. Banks are enabling the customers to conduct some banking services such as account inquiry and funds transfer. Therefore, an audit trail of individual transactions must be kept.[4] The banking applications run by the bank should have proper record keeping facilities for legal purposes (Log of Messages), and all received and sent messages must be kept in both encrypted and decrypted form.[5] Log files provide record of transactions that take place within a system through audit trail and provide timely information as well as authorization of transactions. Evidence from the log files is assembled to resolve the electronically induced financial dispute.

The purpose of documentation is to enable the consumer detect errors promptly and to take action to get the problem resolved and prevent recurrences. Documentation of an electronic payment serves an important evidentiary purpose.[6] Any documentation required by the U.S. EFT Act and Nigerian law is deemed to *be prima facie* evidence that the electronic funds transfer was made. This proof of payment provision is considered essential if consumers are to be adequately protected in an EFT environment. In *Kume Bridget Ashiemar v Gtbank Plc & UBA Plc,*[7] is a case decided by a High Court in Nigeria over an ATM dispense error i.e. a situation where the machine debits a customer's account without actually physically dispensing cash. The plaintiff sometimes in October, 2013 attempted severally to withdraw money from the ATM of 2nd defendant but according to the plaintiff the ATM failed to dispense cash nevertheless her account was debited. The ATM did not dispense cash on each attempt and displayed a message of insufficient funds yet her account was debited. She laid a complaint at her bank, GTB and requested for camera and video recordings of the transactions but none was provided and neither was she refunded the N90,000.00. The court held that plaintiff failed to prove that the ATM of the 2nd defendant (UBA Plc) did not dispense cash to her the various times she attempted to make withdrawals.

In reaching this conclusion the court found that the Plaintiff was not a credible witness because she did not report the alleged failed transactions until after 5 days. The court also relied on the debit entries in Plaintiff's Statement of Account and the entries of PIN entered, Cash Presented and Cash Taken recorded in the 2nd defendant's ATM Electronic Journal logs regarding the plaintiff's withdrawal transactions. The court further reasoned that the documentary evidence namely; the statement of account and ATM Electronic Journal log supersedes the oral evidence of the plaintiff that she did not get money from the ATM of 2nd defendant. In appraising the evidence in the case the court failed to consider the inconsistent entries in the ATM journal logs and the fact that both the 1st and 2nd defendants' witnesses admitted under cross examination that entries or record of transactions in the ATM journal are not always accurate or error proof, meaning that the court ought not to have attached much weight to such a piece of evidence that is not reliable even though it is documentary evidence, which is held to be superior to oral evidence. The court also did not appraise the ATM camera footage presented by the 2nd defendant which did not show the ATM of 2nd defendant dispensing cash and the Plaintiff picking up the said cash. In fact the ATM camera images (still photos and not video recording) were so blurred that one could not make out the person in the photo and whether it was in front of an ATM, let alone the ATM of the 2nd defendant). The court also failed to consider the admission under cross examination of both defendants' witnesses that the Central Bank of Nigeria (CBN) in 2014 directed banks to refund to customers, monies trapped in ATMs

[1] The CBN Guidelines on Operations of Electronic Payment Channels in Nigeria 2016. The Regulation contains Guidelines on **Automated Teller Machine (ATM) Operations**, Point of Sale (POS) Card Acceptance Services, Guidelines on Mobile Point of Sale (MPOS) Acceptance Services, Web Acceptance Services.
[2] Section 2.3 Consumer Protection Framework, 2016.
[3] Guidelines on Automated Teller Machine (ATM) Operations.
[4] See section 1.4.1 2003 guideline on Mobile Telephony.
[5] When stored in encrypted form, it should be possible to decrypt the information for legal purpose by obtaining keys with owners' consent.
[6] See *Kume Bridget Ashiemar v Gtbank Plc & UBA Plc,* Suit No. MHC/198/14, decided by Benue State High Court of Justice in May, 2018 over a dispense error suit.
[7] *Suit No. MHC/198/14*

as a result of ATM non-dispense or partial dispense errors.

The pertinent questions are: How can a bank customer be expected to successfully prove that the ATM of a bank did not pay her cash when she attempted a withdrawal transaction but her account was nevertheless debited and the debit was recorded in her statement of account? On whom should the burden of proof lie in such a case? Who has superior access, control and custody of evidence of a successful ATM withdrawal transaction; the bank customer or the bank? Answers to these questions would reveal that a bank customer does not stand in a position to meet the evidentiary requirements in electronic payment transactions. The plaintiff could not get a refund of her monies trapped in the ATMs not because there is no regulation that mandates a refund but due to poor evaluation of evidence before the court and burden of proof which the plaintiff lacked the ability to discharge in electronic era.

5. Consumers' Liability for Unauthorised Transactions under the U.S. and Nigerian Laws

The U.S. EFT Act provides a basic framework establishing the rights, liabilities, and responsibilities of customers who use electronic fund transfer (EFT) services and financial institutions that offer these services.[1] In dealing with liability from electronic funds transfer, the U.S. EFT Act delineates authorised transactions for which the consumer is fully liable from unauthorised transactions. An electronic funds transfer is commonly initiated by means of an access device such as an ATM card. Where the use of that access is by the customer to whom it was issued or by another person acting under the customer's authority, the ensuing electronic fund transfer is "authorised". A customer to whom an access device is issued by a bank is liable for amounts of all authorised electronic funds.

The EFT Act[2] comprehensively defines an 'unauthorised EFT transaction' as:

> An EFT transaction from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit, but the term does not include any electronic fund transfer (a) initiated by a person other than the consumer who was furnished with the card, code, or other means of access to such consumer's account by such consumer,[3] unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorised, (b) initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or (c) which constitutes an error committed by a financial institution.[4]

There are two main elements in this definition. The first is it must be someone other than the consumer who initiated the transaction without an actual authority to do so and the second is the consumer must receive no benefit from the transaction. Even where the elements of the definition are met, there are certain transactions excluded from the ambit of the definition. In the first case the consumer has voluntarily furnished the third party who has a lawful control of the access device but lacks authority.[5] In the second case the consumer acts fraudulently either alone or together with another person, but does not benefit from the act.[6] However, in the last scenario, an error committed by a financial institution does not render the transaction executed an authorised one and the institution shall assume full liability for such transaction.[7] Effectually, any EFT transaction that falls into one of the first two categories is excluded from being considered 'unauthorised transaction'. The implication of such exclusion is that the transactions are authorised to which a consumer will be fully liable. In any case, an EFT transaction directly initiated by the consumer or one that has been initiated by a third party duly (apparently) authorised by the consumer is deemed to be an authorised transaction.

Specific legal framework on EFT equivalent to the U. S. EFT Act in Nigeria is not in place. Pursuant to the power granted the Central Bank of Nigeria (CBN) under section 2 (d) of the CBN Act[8] and Section 57 of BOFIA,[9] the CBN usually uses circulars and guidelines to regulate electronic payment systems in Nigeria. Provisions pertaining to EFT liability are found in the CBN regulations.[10] The CBN Electronic Guidelines 2003 provides that banks that engage in e-banking should endeavour to insure themselves against risks of unauthorised transfers from

[1] Examples of EFTs covered by the Act are: Automated teller machine (ATM) transfers; Telephone bill-payment transfers; Point-of-sale transfers; Preauthorised transfers from or to a customer's account (i.e., direct deposits or withdrawals of funds); and Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal.
[2] §1693a (11).
[3] Note: In 'furnishing' the access device (i.e., card, code or other means of access), the consumer must have acted voluntarily. Accordingly, where control of the access device is surrendered by the consumer as a result of robbery or fraud, the EFT transaction initiated by the robber or defrauding person is considered to be 'unauthorised'. This was contained in an Official Staff Commentary generously supplied by the Federal Reserve Board of the USA and was effective 2 May 1996. Prior to this interpretation, there was judicial disagreement on what constituted voluntarily furnishing the access device: *Feldman v Citibank*, 443 NYS 2d 43 (Civ Ct, 1981); *Ognibene v Citibank*, 446 NYS 2d 845 at 847 (Civ Ct, 1981); and *State v Citibank*, 537 F Supp 1992 at 1994 (SDNY, 1982).
[4] Electronic Funds Transfer Act, 15 USC § 1693 (1978) and Regulation E, § 205.6 .
[5] Geva, B. (2000), Law of Electronic Funds Transfer, New York p.86.
[6] Ibid p.90.
[7] Ibid p.91.
[8] Central Bank of Nigeria (Establishment) Act 2007 (as amended).
[9] Banks and other Financial Institutions Act, cap B3, Laws of the Federation of Nigeria 2004.
[10] One or two sections of the Cybercrime Act are relevant to the liability issue in this discourse.

customers' accounts, through hacking, denial of services on account of technological failure etc, to adequately insulate themselves from liability to the customers.[1] This regulation recognizes the phenomenon of unauthorised EFT. The section also recognizes fraud as a major component of unauthorised transfers. However, the definition of unauthorised transfers is not given by the regulation or the Consumer Protection Framework 2016 (Framework). The Framework recognizes unauthorised or erroneous debits; financial loss to consumers due to staff negligence/fraudulent activities.[2]

Under §1693(g) EFT Act, consumer liability is limited as follows:

1. Liability no greater than US$50.00 or the amount of the transaction (whichever is less) for unauthorised transactions occurring before notice (of loss or theft of an EFT card and/or PIN) to the institution;
2. Failure to notify the loss or theft of an EFT card and/or PIN within two days of discovery, maximum liability is raised to US$500.00; and
3. If an unauthorised transaction (not previously discovered by a customer) is shown on a periodic EFT account statement, liability is limited to US$500.00 by reporting the discrepancy on the statement within 60 days. Failure to report in 60 days means unlimited liability.[3]

From the above, the financial institution may, in most cases hold the consumer liable for not more than US$50. If the consumer fails to notify the institution within two business days after learning of the loss or theft of an EFT debit card or other access device, however, the consumer can be held liable for up to US$500; and if the consumer fails to notify the institution within sixty days after a periodic statement is sent showing an unauthorised transfer, the consumer bears all liability for any further unauthorised transfers after that time.

The EFT Act limits the liability of the consumer to a certain legal ceiling and allocates liability for unauthorised transfers between the consumer and the financial institution. Such a ceiling is not places on consumer liability in Nigeria. Under the CBN guidelines, consumers must at a minimum, carry out certain responsibilities. Among the responsibilities is the duty to protect financial instruments and information. Consumers must ensure that their personal information such as account numbers, Personal Identification Number (PIN), Bank Verification Number (BVN), access codes, financial instruments including cheques, payment cards are protected. Records of financial transactions such as card receipts, account statements and transaction statements must be safeguarded, disposed or transmitted securely to avoid unauthorised access.[4] It is also the duty of the consumer to report unethical practices, fraud and error. A cardholder has the duties to store the payment card and protect his/her PIN with due care; not to keep his payment card together with the PIN; and not make the payment card available to unauthorised persons.[5] A breach of these duties may result to unauthorised transfers. The cardholder is held liable for fraud committed with his card, arising from the misuse of his PIN or card.[6] The limit of the liability is not stated. It is taken that the liability cannot exceed the sum withdrawn as a result of the fraud. Under the EFT Act, this category of fraud is considered unauthorised transfers and consumers have their liability limited depending on the notice requirements. The liability of the EFT consumer in Nigeria is unlimited. The bank does not bear any loss arising from this risk.

The EFT Act requires that a financial institution must meet three conditions before it can impose liability for unauthorised transfers. First, the access device involved (e.g., the EFT card) must be 'accepted', meaning generally that it must have been requested and received by the consumer before the loss or theft.[7] Second, the institution must have provided a means of identifying the holder of the device; in most cases, through an authentication mechanism such as a PIN.[8] Third, the institution must have disclosed to the consumer the limitations on the consumer's liability under the EFT Act, along with a telephone number and address for notifying the institution of loss or theft. There is no such conditions precedent to imposition of liability on the consumer in Nigeria since banks do not share part of the risk arising from fraud leading to unauthorised transfers.

A U.S. consumer who uses an access device to initiate EFT is required to make prompt notification of loss or theft of the access device or unauthorized transaction that appears on periodic statement of the financial institution to avoid liability arising. The notice should be given within the timeframe indicated under §1693(g) EFT Act. The consumer's notice is effective "when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information".[9] Consumers may give notice in person, by phone, or in writing.[10] Written notice is effective when

[1] Section 3.0 (f).
[2] Section 2.7.3(2) Consumer Protection Framework, 2016.
[3] Most banks in the U.S. set the limit at $200 or $300, and N150, 000 each day in Nigeria, meaning that consumer cannot electronically withdraw more than the amount in cash within a 24-hour period. This protects the consumer by limiting loss in the event card is stolen.
[4] Section 3.2 Consumer Protection Framework, 2016.
[5] Section 2.4.6.1 Guidelines on Point of Sale (POS) Card Acceptance Services.
[6] Ibid, 2.4.6.5. See also Sections 1.4.2(d) Guidelines on Electronic Banking 2003; 3.4.6 Instant Electronic Funds Transfer, 2018.
[7] §1693.
[8] Ibid.
[9] 12 C.F.R. §1005.6(b)(5).
[10] 12 C.F.R. §1005.6(b)(5)(ii).

the consumer mails the notice.[1] For purposes of the limitations on liability under §1005.6, notice provided by a third party on the consumer's behalf is valid.[2] A financial institution may require "appropriate documentation" from the third party to ensure that the person is acting on the consumer's behalf. Section 1005.6(b) (4) of the Regulation requires financial institutions to extend the above time limits for each liability tier if the consumer failed to notify the institution because of "extenuating circumstances." When this occurs, the institution must extend the limits to "a reasonable period of time." [3] In the case of *Bisbey v DC National Bank,*[4] the bank was found liable for not acting following the consumer's notification of an unauthorised EFT transaction. The bank was in fact held liable under the EFT Act for its failure 'to comply with provisions in the Act when addressing a lawful inquiry about possible mistaken fund transfers'. In Nigeria, the consumer has the duty to notify the access device issuer without delay, about missing, stolen, damaged, lost or destroyed card.[5] The use of the phrase "without delay" may be a source of dispute since it is devoid of specificity. Courts may however consider what is reasonable in the circumstance. The notification requirements are not elaborate as that of U.S. Act. One obvious consequence is that financial institutions may not extend the nontice because of "extenuating circumstances."

5.1. Negligence in Assuming Responsibility for Unauthorized Transfer

Negligence or fault relates to the fourth or fifth category of the list of occurrences that may lead to unauthorised transfers stated above. A PIN, any other secret code or password, as well as a private key needed for a digital signature, may be improperly recorded or kept by a customer so as to facilitate breach of confidentiality and availability to unauthorised persons. Short PINs and other codes may be correctly guessed. Similarly, secondary security information, facilitating access to phone banking, such as mother's maiden name or wedding anniversary, may be known to a relative or unfaithful friend who may become an unauthorised user.

Regulation E expressly prohibits the following factors as the basis for imposing greater than is permissible under it.[6] These are the consumer was negligent; an agreement between the consumer and financial institution provides for greater liability; or the consumer is liable for a greater amount under state law. In contrast, EFT initiated by a consumer who acted fraudulently either alone or in concert with other person is excluded from the definition of 'unauthorised transfer' meaning it is authorized EFT for which the consumer will be fully liable. In the U.S. an "unauthorised" electronic funds transfer may be prompted by a customer's negligence, as where the consumer writes the Personal Identification Number on the card or on a piece of paper kept with the card. A person stealing the card with the PIN obtains full control of the access device. In such a case in the U. S., the ensuing electronic funds transfer is nevertheless unauthorised. Consumer negligence under the EFT Act and Regulation E does not alter the liability for unauthorized transfers. Consumer's negligence or carelessness with the EFT card and/or PIN in contributing to an unauthorised EFT transaction is not a factor in determining the consumer's exposure to liability.[7] In other words, a customer may be negligent in using his/her card and may suffer loss when a third party gets hold of the card and transfers money from the customer's account. The U.S. legal position is that, liability of the consumer in this respect ends when he makes a timely notification to the relevant bank. Regulation E prohibits a financial institution from subjecting a consumer to a greater degree of liability for an unauthorised transfer than would otherwise apply because of a consumer's negligent conduct. Consumer's negligent conduct forms part of unauthorised EFT transaction. The Electronic Fund Transfer Act, implemented by Regulation E, is a consumer protection statute, not a law establishing equitable obligations.

The way consumer's negligent conduct is treated in Nigeria differs. The customer's liability for unauthorised transfers may be prompted by a consumer's negligence or fraud. It is statutorily mandated that financial institutions must as a duty to their customers put in place effective counter-fraud measures to safeguard their sensitive information. Where a security breach occurs the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity.[8] That is, the bank has failed to put in place necessary counter-fraud measure as required by the law. Negligence is a relevant factor in consideration of banks liability arising from fraud. section1.4.2 (d) of CBN Guidelines on Electronic Banking in Nigeria, 2003 provides that "banks will be considered liable for fraud arising from card skimming and counterfeiting except where it is proven that the merchant is negligent". The task that saddles the customer with the responsibility of proving negligence on the part of the financial institutions where a security breach occurs is onerous as it is doubtful that the customer would be able to discharge this responsibility.

Indeed, the customer's fault or negligence may have contributed to an unauthorised funds transfer. That is, due to the customer's fault, a person may unlawfully assume control of the card and code, or bypass their use

[1] 12 C.F.R. §1005.6(b)(5)(iii).
[2] Comment 6(b)(5)-2.
[3] Comment 6(b) (4)-1 of the Official Staff Commentary lists hospitalization and extended travel as examples of extenuating circumstances.
[4] 253 App. DC 244, 793 F2d 315 (DC Cir, 1986).
[5] Ibid, 2.4.6.5. See also Sections 1.4.2(d) Guidelines on Electronic Banking 2003; 3.4.6 Instant Electronic Funds Transfer, 2018.
[6] Regulation E 205.6(b)-2 and 205.6(b)-3
[7] Ibid. Staff Commentaries 205.6(b)-2 and 205.6(b)-3)
[8] Section 19(3) of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.

altogether, and initiate an unauthorised transfer. As well, the customer might have failed to advise the financial institution properly and promptly of the loss or theft of either the card or code, or of any other security breach. Or upon receiving notification from the institution of a transfer, the customer may have failed to act diligently and promptly in discovering the lack of authority. The customer may have thereby precluded prompt recourse by the financial institution against the wrongdoer, prior to the latter's disappearance or insolvency, and further enabled that wrongdoer to continue drawing on the account without the customer's authority. Obviously, allocating to the customer losses caused by his or her fault as obtained in Nigeria will enhance consumer diligence and minimize losses. However, loss distribution will not be enhanced.[1] Moreover, litigation regarding the existence of fault and the degree of causation may be wasteful, and worse, may put the consumer, who has fewer resources, in a disadvantageous position.

Fault leading to unauthorised losses may also be attributed to the financial institution. The CBN Consumer Protection Framework, 2016 recognizes financial loss to consumers due to staff negligence/fraudulent activities.[2] Indeed, in the case of a manual signature, the institution's obligation is in detecting the forgery on each instrument, individually. At the same time, in the case of the electronic authentication, the institution is bound to implement a safe system for the distribution of access devices, a safe security procedure for the authentication of payment instructions, as well as an effective system of blocking access upon being advised of loss or theft of the access device.[3] At least historically in English law, banks' liability for payment of forged cheques has been premised on banks being "bound to know the hand-writing of their customers",[4] rather than on a duty of care to detect forgeries. In contrast, in an electronic environment, the institution's duty ought to be premised on negligence.[5] Typically, such negligence is not individual to an institution's employee, as where the latter failed to detect the forgery of a manual signature; rather, in the electronic context, the concern here is with "systemic negligence" by the institution as a whole and on the level of implementing satisfactory computer as well as office procedures. Breach of required standards by the institution, while not necessarily attributable to any individual employee, is nonetheless negligence.[6]In principle, the financial institution's fault may be relevant in two major ways. First, it may be raised as an answer to the alleged fault of the consumer, where the latter is relevant. Second, it is reasonable to expect that where the institution seeks to be justified in acting on the basis of an agreed-upon security procedure, namely, in carrying out transfers where a PIN, any other secret code or password, private key needed for a digital signature, is improperly recorded or kept by a customer so as to facilitate breach of confidentiality and availability to unauthorised persons, the security procedure set up by the financial institution must be safe, sound, and reliable, and that no negligence occurred in its conducting of the verification procedures.[7] In *Pickman v Citibank*,[8] the bank was found liable, despite the consumer not reporting losses for 3 months (beyond the required notification period maximum of 60 days), but because the consumer successfully put the integrity and security of the bank's EFT computer system into question. The court decided the issue 'in favour of the human, rather than the machine' quoting 'to err is human'.[9]

5.2 Liability of Financial Institutions

The EFT Act under § 1693h provides for liability of financial institutions due to failure to complete an EFT or for failure to act properly causing damages as follows:

… a financial institution shall be liable to a consumer for all damages proximately caused by—

(1) the financial institution's failure to make an electronic fund transfer, in accordance with the terms and conditions of an account, in the correct amount or in a timely manner when properly instructed to do so by the consumer, except where—

(A) the consumer's account has insufficient funds;

(B) the funds are subject to legal process or other encumbrance restricting such transfer;

(C) such transfer would exceed an established credit limit;

(D) an electronic terminal has insufficient cash to complete the transaction; or

(E) as otherwise provided in regulations of the Board;

(2) The financial institution's failure to make an electronic fund transfer due to insufficient funds when the financial institution failed to credit, in accordance with the terms and conditions of an account, a deposit of funds to the consumer's account which would have provided sufficient funds to make the transfer, and

[1] Ibid, p.231.
[2] Section 2.7.3(2) Consumer Protection Framework, 2016.
[3] The financial institution may also be charged with a duty to ensure the safety and security of public-access terminals. For example, section 1.0 of Guidelines on Electronic Banking in Nigeria charges financial institutions on Technology and Security Standards.
[4] *Smith v. Mercer* (1815), 6 Taunt 76 at p. 86, 128 E.R. 961 at p. 965, Heath J.
[5] Geva, Benjamin (2003), op cit, p. 231.
[6] Ibid.
[7] Ibid. 232
[8] 443 NYS.2d 43 (Civ Ct City of NY, 1981).
[9] Ibid.

(3) The financial institution's failure to stop payment of a preauthorized transfer from a consumer's account when instructed to do so in accordance with the terms and conditions of the account.

There are two acts that can justify inability to transfer funds in accordance with the customer's mandate. These are an act of God and a technical malfunction which is known to the consumer. In this respect the EFT Act under § 1693h provides:

A financial institution shall not be liable under subsection (a) (1) or (2) of this section if the financial institution shows by a preponderance of the evidence that its action or failure to act resulted from—

(1) An act of God or other circumstance beyond its control, that it exercised reasonable care to prevent such an occurrence, and that it exercised such diligence as the circumstances required; or

(2) A technical malfunction which was known to the consumer at the time he attempted to initiate an electronic fund transfer or, in the case of a preauthorized transfer, at the time such transfer should have occurred.

The EFT Act protects the consumer from liability when an electronic payment to a third party is not completed as directed by the consumer. For example, if a consumer uses a home banking system to order payment of an electric bill but the institution fails to make the payment, the institution becomes liable to the consumer for all damages proximately caused by the failure to make the payment correctly.[1] Mistakes are likely to occur during the operation of an e-banking transaction. Under the EFT Act, 1978, if a consumer has authorised a third party to initiate a series of electronic debits to the consumer's account, the consumer may stop payment of such a preauthorised debit any time up to three business days before the scheduled date of the debit. If an institution receives a stop-payment order but fails to stop the debit, the institution is liable to the consumer for all damages proximately caused.[2] The apparent weakness in the EFT Act is that it does not provide a stop-payment right for other types of electronic payments, such as EFT debit card transactions. In Nigeria, there is very little scope for the banks to act on stop payment instructions from the customers in e-banking. This notwithstanding, banks should clearly notify the customers the time frame and the circumstances in which any stop-payment instructions could be accepted.[3] In case a customer complies with the bank time frame and fails to act on customer's stop payment instructions, liability of the bank is not indicated under any CBN guidelines.

The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 makes the financial institution to hear liability where there is a breach of duty to put in place effective counter-fraud measures to safeguard the customer's sensitive information.[4] Where there is a breach of this duty, the Act makes provisions for restitution for any loss suffered by a person on account of electronic fraud. In addition to any other penalty prescribed under this Act, the Act mandates courts to order a person convicted of an offence under the Act to make restitution to the victim of the false pretense or fraud by directing the person convicted to pay to the victim an amount equivalent to the lost sustained by the victim where the property involved is money; and in any other case to return the property to the victim or to a person designated by him; or pay an amount equal to the value of the property, where the return of the property is impossible or impracticable.[5] Section 37 the Cybercrime Act places certain duties on financial institutions in Nigeria in relation to their customers. Relevant to the liability issue is the duty to provide clear legal authorization for a debit or to reverse the debit within 72 hours where a customer notifies the financial institution of an unauthorised debit on its account.

Banks will be considered liable for fraud arising from card skimming and counterfeiting except where it is proven that the merchant is negligent.[6] Acquirers[7] should reconcile and refund all funds in their possession, belonging to customers as a result of ATM's non-dispense and partial dispense errors. Acquirers should also install appropriate mechanism to immediately initiate refunds without the prompting of the issuing bank or the customer.[8] Experience has shown that where there is an ATM debit without dispensing physical cash, the customer's account is immediately credited. However, there still exist instances where refunds are not made on the spot. Delay is often experienced in resolving the problem that arises thereafter.

The CBN Regulation on Instant (Inter-Bank) Electronic Funds Transfer[9] Services 2018 covers liability for

[1] In the UK, a bank which has made a payment under a mistake of fact is *prima facie,* entitled to recover the payment- *Barclays Bank Ltd v. W.J. Simms Son & Cooke [Southern] Ltd* [1979] 3 All E.R.522, see also *Lloyds Bank Plc v. Independent Insurance Company Ltd* [1999] 2 WLR 986.

[2] See § 1693e., of the EFT Act, 1978.

[3] Section 3.0 (E) Electroniic Guidelines 2003.

[4] Section 19(3) of the Cybercrimes (Prohibition, Prevention, Etc) Act, 2015.

[5] The Cybercrime (Prohibition, Prevention Etc) Act 2015 contains offences relating to electronic transactions. These offences include theft of electronic devices, fraudulent issuance of e-instructions, identity theft and impersonation, manipulation of ATM/POS Terminals, Phishing, spamming, spreading of computer virus, dealing in card of another, purchase or sale of card of another and use of fraudulent device or attached e-mails and websites.[5]The Act comprehensively provides sanctions for these offfences since criminal liability is the main aim of the Act. Section 33 specifically deals with all forms of Electronic cards related fraud and provides sanctions.

[6] See section1.4.2(d) of CBN Guidelines on Electronic Banking in Nigeria, 2003.

[7]Acquirer means bank or any other legal person concluding contracts with merchants concerning acceptance of payment by means of an electronic payment token.[7]

[8] Section 1.3(v) and (w) Guidelines on Automated Teller Machine (ATM).

[9] Instant (Inter-Bank) EFT or Instant EFT or Instant Payment means Instant EFT Payments system between two distinct entities when delivery

wrong transfer due to bank error.[1] where a Sending Entity[2] erroneously sends value contrary to customer's instructions due to wrong account number, wrong amount, duplication, etc to a Receiving Entity[3] and requests the reversal in writing within 14 working days of the transaction, the Receiving Entity must oblige within one (1) business day without recourse to the customer (beneficiary) of the Receiving Entity provided funds are available. An automatic indemnity is inferred against the Sending Entity making the reversal request. Where funds are not available, the Receiving Entity must immediately notify its customer that the account was wrongly credited and provide proof of such notification to the Sending Entity. The Receiving Entity then notifies the customer the consequences of not funding the account within 24 hours, which includes watch-listing in the banking industry, Credit Bureau and reporting to law enforcement agencies. The Receiving Entity would watch-list the customer if he fails to provide fund within seven (7) days The Receiving Entity shall refund the transaction as soon as funds are either partially or fully available.[4]

Transfer recall due to customer error deals with situations where a customer claims to have made a transfer in error.[5] The Sending Entity has the duty to encourage the complainant to contact the beneficiary for an amicable settlement where the beneficiary is known to the complainant. Where the beneficiary is not known to the complainant or a known beneficiary refused to effect a refund to the complainant, the Sending Entity having received a tenable claim from customer must notify the Receiving Entity who would place a lien on the amount in the account of the beneficiary and thereafter obtain the consent of the beneficiary to execute refund. Where the beneficiary does not give consent, the internal auditors of the Sending and Receiving Entities then mediate between the two customers within 2 weeks of the complaint to resolve the issue, and their decision is final. The lien on the amount in the beneficiary's account should not last more than 2 weeks. Where the contested beneficiary has utilized the fund such that lien could not be placed, and he/she refuses to fund the beneficiary account to facilitate refund, the Receiving Entity's Internal Auditors watch-list the customer's BVN and the Sending Entity may report the incident to law enforcement agencies.[6]

The EFT Act under § 1693f provides for error resolution. The provision requires institutions to investigate and resolve a claim by a consumer that an error has occurred, such as when an EFTPOS debit card payment to a merchant is shown on the statement as $200 while it should have been $20. The institution may complete the process within ten business days after receiving notification from the consumer; alternatively, it may provisionally credit the consumer's account for the amount of the alleged error within ten business days and then take up to forty-five calendar days to resolve the matter.[7] Procedure for Complaints Redress is also contained in almost all the Regulations.[8]

7. Conclusion

Regulation of banking business has always been driven by the desire to protect consumers and to prevent fraudulent transactions in the customers' accounts. Generally, flaws in e-banking may cause huge financial losses to consumers and financial institutions transacting banking business in electronic form. Whenever these risks eventuate, liability must be apportioned among parties to e-payment. The complex facets of EFT regulation therefore concern the extent to which consumers need or deserve to be protected from third party fraud, faults on the part of financial institutions, and consumers' own carelessness. Consumer protection legislation seek to reduce uncertainties for both consumers and financial institutions regarding liabilities related to electronic payments, provide protection against unauthorized or erroneous electronic transactions that access consumer accounts by setting guidelines to allocate liability for unauthorized transactions as well as imposing documentation and record-keeping requirements to assist in detecting and remedying disputed EFT. In the United States, the EFT Act was enacted specifically for the regulation of electronic funds transfers. The EFTA protects individual consumer rights and defines the rights, liabilities and obligations of parties to an electronic funds transfer. The consumer is required to meet some conditions to benefit from the protection of the law. Similarly, a financial institution must meet its duties so that a consumer shares losses arising out of unauthorised transactions. Arguably, allocation of liability is the result of balance of the duties of the consumer and financial institutions in the US**.** The Rights, liabilities and

from the Sending Entity to the Receiving Entity takes place within 1 minute (60 seconds). A payments system where delivery to the Receiving Entity occurs beyond 1 minute is considered to be an ACH system.

[1] Section 10.2 3 Regulation on Instant (Inter-Bank) Electronic Funds Transfer Services 2018.

[2] Sending Entity shall mean a Nigerian company or Financial Institution licensed by the CBN to carry on the business of facilitating Electronic Funds Transfer services in Nigeria and who initiates an Instant EFT on behalf of its customers. See section13.4 Regulation on Instant (Inter-Bank) Electronic Funds Transfer.

[3] Receiving Entity shall mean a Nigerian company or Financial Institution licensed by the CBN to carry on the business of facilitating Electronic Funds Transfer services in Nigeria and who receives the proceeds of Instant EFT on behalf of its customer. See section13.5 Regulation on Instant (Inter-Bank) Electronic Funds Transfer.

[4] Section 10.2.

[5] Regulation on Instant (Inter-Bank) Electronic Funds Transfer Services 2018, section 10.4.

[6] Section 10.4.

[7] See the EFT Act, § 1693f.

[8] See section 10 Regulation on Instant (Inter-Bank) Electronic Funds Transfer Services; section 2.7 Consumer Protection Framework.

obligations of the consumer and bank in respect to the electronic bank transfer are spelt out clearly and cannot be taken away by the contract between banker and customer.

The U.S. adopts a legislative and self-regulation approach using the EFT Act and Regulation E. Nigeria has no single comprehensive legislation equivalent to the US EFT Act. While the U.S. EFT comprehensively covers present and future innovations in the electronic payment world, the CBN regulations deal with the payment channels piecemeal. The EFT Act and Regulation E create a concise, three-tier structure for calculating consumers' liability for unauthorised EFT transactions. There is certainty in allocation of risks under the EFT Act. Of importance is the issue of consumer negligence in the use of EFT access devices. The negligent conduct of the customer is regarded under the EFT Act as unauthorised and for the simple reason of the third party being in unlawful control of the access device at the time of transaction. Consumers bear alone liability for negligent conduct in Nigeria. Subject to certain exceptions, a financial institution is liable to a consumer for all damages proximately caused by the financial institution. The refund arrangement put in place in Nigeria does not fairly allocate risk between the consumer and financial institution in the absence of proximate damages. There is no limit to consumer EFT liability as a result of unauthorized including negligence. Consumers' liability is unlimited. It is concluded that the protection accorded consumer by the EFT Act is wider and financial institutions share more liability than the consumer as opposed to the situation in Nigerian law.

The legal and regulatory framework for electronic Payment System in Nigeria is contained in CBN guidelines[1] and a few statutes.[2] This is fragmentary. Nigeria should enact legislation equivalent to that of U.S. and supplemented by proactive CBN regulations. The National Assembly should pass National Payment Act that regulates EFT. Overall financial regulatory frameworks should seek to implement e-payment-related rules in a coherent manner. The proposed law should as well establish clear and fair liability regime between consumers and financial institutions. Global best practices necessitate the enactment of a National Payment System law which provides legal framework for the administration and operations of the payment system. Thus many countries, both developed and developing have enacted National Payment Act.[3]

The transactions that form unauthorised EFT should be statutorily stated to include among other things, the incidents of the ATM cardholders being forced by thieves to withdraw funds from their accounts through a public access terminal, and consumer negligent conduct. These should be taken as unauthorised access as obtained in the U.S. The insurance cover mandated by the CBN regulation should be made by the financial institutions to cover such loss. It is important that this issue is addressed by law. It is not enough that the banks be considered or be allowed to consider themselves discharged of the obligation by the provision of secure ATM points, and regulating the use of the cardholders PIN. Obviously, allocating to the customer losses caused by his or her fault as obtained in Nigeria will enhance consumer diligence and minimize losses. However, loss distribution will not be enhanced. Moreover, litigation regarding the existence of fault and the degree of causation may be wasteful, and worse, may put the consumer, who has fewer resources, in a disadvantageous position. The alternative is loss sharing between the customer and the institution - that is, to allocate to the consumer losses only up to a low threshold, irrespective of fault, thereby enhancing diligence without causing the consumer undue hardship. This can be done by either statute or agreement.

Technology is constantly advancing and banks being better placed than individuals need to keep abreast of the latest security systems in the battle against technology based frauds. Financial institutions must as a duty to their customers put in place effective counter-fraud measures to safeguard their sensitive information. The burden of proof of negligence placed on the consumers by the Nigerian law in relation to occurrence of security breach on part the financial institutions is onerous. The financial institution stands in a better position to prove that it was not negligent and that it did a lot more to safeguard its information integrity. The consumer should not be saddled with the burden of proof in the circumstance. The provision should be amended to shift the burden to the financial institutions.

Akshada, K., Chhajed, K,. and Kapse, A. (2017) Review on Fraud Detection in Electronic Payment Gateway, *International Research Journal of Engineering and Technology (IRJET)* 04 (01) p. 841.
Arora, A., (1988), Electronic Banking and the Law, IBC Publishing.
Bergman, B. (2005), "E-fraud – State of art and countermeasures" http://www.ep.liu.se/exjobb/ida/2005/dd-d/029/ accessed December 15, 2018.
Board of Governors of the Federal Reserve System of the USA, *Report to Congress on the Application of the Electronic Funds Transfer Act to Electronic Stored-Value Products* (1997).
Bohm, B., and Gladman, (2000), "Electronic Commerce: Who Carries the Risk of Fraud?" *The Journal of*

[1] Such as Guidelines on Electronic Banking, Consumer Protection Framework, Regulation on Instant (Inter-Bank) Electronic Funds Transfer Services and Guidelines on Operations of Electronic Payment Channels in Nigeria.
[2] See the Cybercrime Act 2015.
[3] See for examples Zambia National Payment Act, 2007; Kenya National Payment Act, 2011; Ghana National Payment Systems Act, 2003. The Nigeria National Assembly has not passed the National Payment System Bill (NPSB) pending before it. A similar bill is the Payment System Management Bill 2017.

Information, Law and Technology.

Ekwueme, C., Egbunike, P., and Amara O. (2012), "An Empirical Assessment of the Operational Efficiency of Electronic Banking: Evidence of Nigerian Banks" *Review of Public Administration and Management 1(2)* 377.

Ellinger, E., *et al.,* (2011), Modern Banking Law p. 562; Sappideen, R., (2003) "Cross-border Electronic Funds Transfers through Large Value Transfer System, and the Persistence of Risk", *Journal of Business Law* 13 584.

Federal Bureau of Consumer Affairs (Australia), *A Cashless Society? Electronic Banking and the Consumer* (1995).

Awareness of security risks by financial institutions and consumers' education play an important role in reducing fraud in e-payments. Financial institutions should be aware of the types of fraud, statistic and best practices. Consumer awareness and education is important in order to reduce identity theft or payment data theft. This would help the user in adopting active and cautious attitude when doing transaction using internet. It could teach them to be aware of possible risks, avoid e-scams, and minimize giving information to merchants when buying online. This would increase consumers' responsibility in keeping personal data secured in physical and virtual world. Customers should also be educated on the necessary security systems to have in place on their part. Victim Assistance Services providing clear methods for notification of any unauthorized transaction and immediate incident response to minimize the loss.

References

Geva, Benjamin. (2003) "Consumer Liability in Unauthorized Electronic Funds Transfers" *Canadian Business Law Journal* 38 (2) 207.

Graham, T. (2002), "Dispute resolution: E-Fraud and Jurisdiction", http://www.tjguk.com/topical/litigation/efraud_and_jurisdic tion_winter2001.html accessed December 15, 2018.

Graycar, A and Smith, R. (2002), "Identifying and Responding to Electronic Fraud Risks", Australian Institute of Criminology, http://www.aic.gov.au/media_library/conferences/other/graycar_adam/2002-11-registrars.pdf accessed December 15, 2018.

Hariom, T. , and Abhishek, S. (2016) "The Study of Electronic Payment Systems", *International Journal of Advanced Research in Computer Science and Software Engineering* 6 (7) 297.

Imafidon, A., (2013), "Challenges of E-banking and Payment Systems in Nigeria" *Journal of the Chartered Institute of Bankers of Nigeria.*

Joseph, C., and Geraldine, E. (2017), "Internet Banking: Identity Theft and Solutions - The Nigerian Perspective *Journal of Internet Banking and Commerce,* 22, (2) , 1 p. 4.

Kethi, D. (2007) "An Analysis of the Legal Challenges posed by Electronic Banking", *Kenya Law Review* (1) 323.

Mark, H., QC,(2002) Paget's Law of Banking ed, Butterworths, London.

McCarthy, J., (2002), "Consumer Protection in Contemporary Electronic Payment Systems:- A Familiar Wolf in Digital Clothing?" *C.O.L.R.* II, www.ucclawsociety.com/colr/editions/2002/2002- 2.pdf, accessed on 28 December, 2018.

Niranjanamurthy, M., and Dharmendra, C. (2013) "The study of E-Commerce Security Issues and Solutions", *International Journal of Advanced Research in Computer and Communication Engineering* 2 (7).

Omotubora , A., and Subhajit , B. (2018), " Regulation for E-Payment Systems – Analytical Approaches Beyond Private Ordering", *Journal of African Law*, 62 (2), 281.

Procter, L. (1993) "Reforming the Australian Payments System: The State of Play" *The Australian Banker (*3) 135.

Rashad, Y., and Abu Bakar, S.(2011), "Electronic Banking Fraud: The Need to Enhance Security and Customer Trust in Online Banking", *International Journal in Advances in Information Sciences and Service Sciences* ,310 (61)505 pp. 505-506.

Reed, C.(1994) "Consumer E-banking", 11 JIBL 451.

Report of the Electronic Commerce Steering Group, "Approaches to Consumer Protection within APEC Region" October 2002, www.nacpec.org/docs/Approaches_to_consumer_protection.pdf. accessed on 28 December, 2018.

Richard, J. (2010) The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy Workshop on the Economics of Information Security Harvard University.

Tyree, A. "Mistaken Internet Payments", ttp://austlii.edu.au/~alan/mistakenepayments, html, accessed December 15, 2018.

Vincenzo, S. "Digital Signature Legislation in Europe: Virtual Banking and Electronic Payment", Sept International Bar Association 2000 conference, The Netherlands.

White, P. (1997) "A Critique of the Self-Regulation of Electronic Funds Transfer in Australia" (M Bus Minor Thesis, Victoria University of Technology.

White, P., and Islam, S. (2008), "Formulation of Appropriate Laws: A New Integrated Multidisciplinary Approach and an Application to Electronic Funds Transfer Regulation, Berlin: Springer-Verlag Berlin Hedelberg.