# An Analysis of the Legal Challenges posed by Electronic Banking

Kethi D. Kilonzo*

## 1. LEGAL DEFINITION: WHAT IS ELECTRONIC BANKING?

If you are selling water in the desert and it starts raining, it is time to change your business model.[1] The future of banking lies in clicks and mortar. Paper based systems are slow, labor intensive and correspondingly expensive to maintain hence, the growth of electronic funds transfer systems.

In the eyes of the unenlightened, electronic banking is the same as internet banking. This is a misconception. Any statement equating electronic banking with Internet Banking is a factual misstatement. 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).[2] However, there is no universally accepted legal definition of an electronic funds transfer. Since it is the privilege of the writer to create her own dictionary, "electronic funds transfer" "electronic banking" as used in this article, means, "any transfer of funds initiated or processed using electronic techniques."

In its definition of banking business, the Banking Act[3] only refers to the cash and cheque payment systems. The Act provides no definition and makes no reference to electronic banking. Electronic Commerce (and electronic banking) preceded the Internet. Before the advent of communication through Internet, business communication was conveyed using telex, facsimile machine, telephones, telegrams and other electronic media.

The Internet is a decentralized information distribution network accessible by computer. There is no central authority through which information must pass. It operates through independently functioning computer systems that are connected by communicating in a common protocol or language.

The Internet is also unregulated. It operates twenty-four hours a day, can be instantly accessed, is inexpensive and contains information that is downloadable for future reference.[4] Electronic commerce preceded

* The writer is an Advocate of the High Court of Kenya, associate at Kilonzo & Company Advocates & a Financial Consultant with Finclegal Ltd.

Internet. Before the advent of communications through internet, business communication was conveyed using telex, facsimile machine, telephones, telegrams and other electronic media. With the emergence of the Internet, two stages in the development of electronic commerce may be identified: the traditional and the modern stage. In the traditional stage, the networks were means for moving data, in the modern stage, the networks (and internet being their synthesis) are the market.[3]

Money and payment play a central role in commercial and financial transactions. Every working day millions of transactions are concluded involving the sale and purchase of land, goods and services, the lending and borrowing of money, and the issue and transfer of financial instruments. Every working day funds are transferred and payments made in discharge of money obligations. Save for small value transactions, payment, and banking go hand in hand.

It is necessary to identify how electronic banking actively interferes in the lives of thousands of consumers who use banking products to manage their economies. Banking is not simply about cheap delivery – one of the benefits of electronic banking – running a bank is not like selling books or mobile telephone handsets. There is a whole range of other types of risks – credit liquidity, interest rate risk, and market risk that need to be taken into account. Brand name in banking is one of a bank's (and most enterprises') most important assets. Customers will feel more comfortable with a name that they know, and perhaps one whose name they see everyday in the street on signs above physical bricks and mortars (building) and not so much the provision of electronic; or other user-friendly banking facilities.

The Simplicity of the emphasis on banking at the click of a mouse, 24 hour banking, banking at your finger tips, mobile banking, belies the intricacies, dexterity and network of relationships involved in the banking relations between banks themselves, banks with corporate as well as natural personalities, banks and national governments and banks in the international environment.

In the eighteenth century before cheques came into common use, the principal characteristics of banking were that the banker accepted the money of others on the terms that the persons who deposited it could have it back again from the banker when they asked for it, sometimes on demand, at other times on notice, according to the conditions agreed at the time of the deposit, and meanwhile the banker was at liberty to make use of money by lending it out at interest or investing it on mortgage or otherwise.

From the nineteenth century into the twentieth century, money is now paid and received by cheques to such extent that no person can be considered a banker unless he handles cheques as freely as cash. It is during this particular era that technology has become widespread and its effect in the financial sector inevitable. Technology has facilitated electronic commerce, which has in turn relied heavily on the presence of a stable and secure means of payment.

Payment and banking go hand in hand. Electronic Banking is complementary to, and a manifestation of electronic commerce, for the simple reason that electronic commerce requires a payment system that is easily and readily processed. Cheques and paper based payment systems are more often than not deferred payment systems and consequently ill suited to electronic commerce.

Banking has undergone a revolution on the inception of technology into the industry. Though the relationship of the bank and its customers remains contractual, the terms of these contracts have taken 360 degrees turn around.

A good illustration will be the Judgement of Lord Atkins in the celebrated case of *Joachimson vs Swiss Bank* (1921).[4] He describes the relationship between the bank and its customers as one and the same contract involving obligations on both sides and includes the following conditions:

- The bank undertakes to receive money and to collect cheques for its customer's account;
- The proceeds so received are not to be held in trust for the customer, but the bank borrows the proceeds and undertakes to repay them;
- The Promise to repay is to repay at the branch of the bank where the account is kept;
- It includes a promise to repay any part of the amount due against the written order of the customer addressed to the bank at the branch;
- Such written orders may be outstanding in the ordinary course of business for two or three days;
- The bank will not cease to do business with the customer except upon reasonable notice;
- The customer undertakes to exercise reasonable care in executing her written orders so as not to mislead the bank or facilitate forgery, and;

- The bank is not liable to pay the customer the full amount until he demands payment from the bank at the branch at which the current account is kept.

Eighty-five years after the pronouncement of this Judgement, electronic banking provides consumers with among others the following benefits.

- Twenty-four-hour access to their accounts;
- Payments need not be made upon written orders;
- Widespread use of digital signatures;
- Payments may be made through public access terminals, for instance Automated Teller Machines;
- Electronic pay roll systems
- Direct transfers
- Electronic cheques and so on.

## 2. CONSUMER ELECTRONIC PAYMENT SYSTEMS

Electronic payment systems exist in a variety of forms, which can be divided into two groups: consumer activated systems and non-consumer activated systems[5]. 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 consumer customers, that is personal account holders, do not have similar direct access. They include transactions initiated among and between banks, corporations, governments, and other service firms.[6]

Consumer activated or retail electronic systems encompass transactions involving personal account holders as opposed to corporate account holders. There are several kinds of electronic funds transfer services available to personal account holders:

- Pre-authorized recurring payments from consumers' accounts to those of creditors, such as mortgage or insurance companies (debit transfers), as well as to consumers' accounts from those of debtors, such as in payment of wages, salaries or benefits (credit transfers);
- Storage devices, such as stored value cards, which may be used to transfer funds from a consumer to a merchant at the point of sale;
- Electronic cheques

- The use of Internet to pay consumer bills, such as electronic cash, Internet payment products and electronic bill payment services
- Public Access Automated Teller Machines (ATM's) enabling consumers to withdraw cash, make deposits, transfer funds from one account to another, and pay bills and providing twenty four hour banking services.
- Point of sale terminals at Merchant's places of business enabling consumers to transfer funds to Merchants in payment of goods and services purchased at Merchant's places of business.
- Telephone or home terminals at consumers' homes facilitating inter-account transfers, bill payments, and the payment for goods and services purchased from the consumer's home.
- Mobile Banking

Automated Teller Machines (ATMs) provide many more services than simple dispensing cash. ATMs have evolved from simple note distributors to true mini branches where the customer can pay bills, verify checking account balances and obtain statements. Kenya Commercial Bank, Barclays Bank and Standard Chartered, National Bank of Kenya, Commercial Bank of Kenya, Co-operative Bank of Kenya are among Banks in Kenya that have public access automated teller machines. And the list is growing longer by the day.

The facilities offered by Standard Chartered via their public access terminals, are by far the most advanced in the market. Standard Chartered was the first bank to install ATMs in the market. The Bank's ATM cardholders may:

- Access their accounts twenty-four-hours a day, 7 days a week, 365 days a year, from any Standard Chartered ATM facility located countrywide or worldwide. They may also access their accounts in a similar manner, but an extra cost, at any ATM facility, other than a Standard Chartered ATM, that displays the VISA Logo, and located in the country, or anywhere else on the globe.
- Order a cheque-book;
- Order a bank statement;
- Withdraw cash
- Deposit cash or cheques at select ATMs;
- Initiate the transfer of funds to the account of a third party, for example, the payment of electricity bills;
- Transfer of funds from one account to another belonging to the card-holder, whether the branch at which any or both of the accounts are opened, are located within or outside his country's national frontiers;

- Instruction deposit, that is, the deposit of paper-based payment instructions via the ATMs.

## Digital Signatures

The digital signature has received legislative recognition in Europe under the auspices of the European Union, and also in the United States. The use and/or legal validity of the digital signature remain unregulated in Kenya.

The use of digital signatures is indispensable in the conduct of electronic banking. This mode of banking necessitates, and demands, the replacement of personal relationship management with man-to-machine interaction. The use of electronic media, be it in electronic commerce or electronic banking is incompatible with the delivery and use of written records.

The use of digital signatures within the electronic banking environment assumes the character of message authentication. This is a procedure between two parties, which allows each party to verify that data received electronically is genuine and has not been altered. The message authentication code is in fact a security procedure applied to electronic payment systems. As message authentication operates in a closed environment within a particular bank, its use is regulated by the bank and particularly in the agreement between the bank and it's customer.[7]

Though deemed and designed to serve as an electronic signature, it is an open-ended question whether the Personal Identification Number is an electronic signature within the remit of the law. In Europe, and particularly, under the auspices of the European Union it falls outside digital signature laws, whereas in the United States digital signature laws empower parties to a transaction to choose the type of electronic signature, which will bind the parties thereto. The definition of electronic signatures in both jurisdictions embraces the whole arena of electronic commerce.

As the use, validity and the evidentiary value of electronic signatures remain unregulated in Kenya, it may be said that the parties to an electronic contract regulate its use. Its legal validity, however, remains untested. This is indeed a legal vacuum, and particularly within the banking environment, because the customer's signature is his mandate to the bank; further, cheques and hand written signatures go hand in hand and are regulated by legislative enactments.

The use of signatures other than written signatures is certainly not a new legal development. Mechanical devices used to affix signatures or seals have been given legal effect in the documents where the signatory is a corporation and not a natural person. A rubber stamp is commonly affixed on a written document and though the affixation is mechanical, there is documentary evidence of a signature. Seals or other marks affixed by mechanical devices are however not digital signature because of their affixation on written documents.

In contrast, digital signatures are affixed on digital documents or records. Both the signature and record are sent over telecommunication lines. There is no physical evidence at all. A good example is the use of a card and a personal identification number to effect an electronic payment to a third party through an automated teller machine. The use of the card and the Personal Identification Number by the cardholder serves as a mandate by the bank to debit his account with an amount and debit the account of the third party with the same amount. The mandate thus becomes the digital signature of the payer. The terminal receipt, the output of the transaction, may serve as a documentary evidence of the payment to the third party. However, in all cases, there is no tangible evidence of the input of the digital signature and subsequent payment message by the cardholder.

The digital signature is an essential component of electronic commerce. This is in large part due to the need to address the authentication, non-repetition and message integrity.

A digital signature should identify the holder thereof and warrant the integrity of the document to which it is attached. In addition, it should be created by a device that the signatory can keep under his exclusive control.

The mandate is fundamental in the banker customer relationship. Within the wide range of paperless transfer, it poses a number of questions. Can a signature effectively verify an electronic transmission, and will such transmission make it harder to see alterations? How effective legally is a replacement of the customer's signature by his Personal Identification Number?

As a rule, instructions given to the bank by its computers are authenticated by means of security procedures. The instruction to the bank is the customer's mandate and is communicated through electronic means. The security procedure herein is analogous to a digital signature for it constitutes

the bank's authority to execute the mandate. Further, the digital signature is equivalent to the signature in cheques in so far as both facilitate the processing of the payment message by bank.

In consumer activated electronic funds transfer systems, cards and Personal Identification Numbers 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 and 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 to consequential loss, which may be substantial where a wrongful debit left the account with insufficient funds to meet valid payment instructions, which were consequently dishonored. To this end, the confidential personal identification number was designed to serve as an electronic signature.[8]

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.[9]

Digital signatures are indispensable to electronic banking. 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 not expressly provided for in the agreement between him and the bank, but may of necessity be implied by a court of law in to the contract.

A law regulating electronic signatures would ensure that they are legally recognized and that they are admissible as evidence. Consequently, digital signatures will not be denied legal validity, effect, or enforcement solely on the grounds that they are in the form of electronic data. They will be recognized in the same manner as hand written signatures.

The use of digital signatures is not peculiar to banking. Indeed, lawmakers in Europe and USA and other jurisdictions like Latin America have enacted legislation regulating digital signatures in the natural context of contract law and in particularly electronic commerce. The United Kingdom's Law regulating the use of digital signatures, on the Electronics Act, 2000 received royal accent in 2000 when the Queen digitally signed the enactment.

These jurisdictions have recognized the potential stimulants of electronic commerce in the conduct of business and the adjutant need to secure transactions over open network through the use of digital signatures.

If the regulation of digital signatures were to become a reality in Kenya, such regulation should be universal that is to say across the board, and not industry specific. It should not be limited to the banking sector.

## 3. DOCUMENTATION OF ELECTRONIC FUNDS TRANSFER

The documentation of electronic funds transfers is very important. Due to the nature of electronic banking, that is, the man to machine interaction, the bank customer is entitled to receive at the end of the transaction confirmation that his account has only been credited by the amount of the transaction authorized by him through the input of his Personal Identification Number. A terminal receipt is therefore required at any time an electronic transfer 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 who initiated the transfer, the time and the balance in the consumer's account.

It is a breach of the bank's obligations to it's bank customers not to produce the above receipt. Such failure is made worse by the fact that a similar transaction over a bank-hall counter will in all occasions be evidenced by an audit trail. That is, there will be written receipts and/or paying slips written by both the bank and the customer.

Documentation of electronic funds transfer remains unregulated in Kenya. The Bank's obligation to provide a terminal receipt (advice slip) is an implied term of the contract between the cardholder and them. In the United States, production of a receipt at an ATM is regulated, and, forms part of the contract and cannot be misapplied by the parties of the contract. Breach of that obligation invites legal liability. However, the bank can raise defences of power failures, paper jams and the like, as long as it can prove that such situations are not the norm, but rather the exception.

Further, it is only fair that regular bank statements supplement the receipt evidencing the electronic funds transfer at terminal or any other transaction by issuing cyclical statements of account. 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 into place. Banks offering electronic banking facilities need to convince

customers that their deposits are safe and secure.

It is the bank's duty to issue regular bank statements so as to enable a consumer to verify any unauthorised electronic funds transfer. The Customer on the other hand has a duty to promptly verify its correctness.

The failure of the bank and its customer to discharge their duties invites different consequences. There is disparity of the liability accruing of the parties in the United Kingdom and in the United States. In the United Kingdom the obligations of the parties are governed by Common Law. The customer is under the obligation to verify the contents of the bank statement; however, the bank has an obligation to send such a statement. The recurrence of the statement is a matter for agreement between the parties. It is arguable whether this would be the legal position in Kenya. It is however, the practice.

In the United States, the customer must, within sixty days, inspect the statement and report any errors or unauthorized withdrawals to the bank. On the other hand, the bank must send a statement in every month there is an electronic funds transfer, and if there are no such transfers, a quarterly statement. This requirement is peculiar to electronic payment facilities.

Documentation of an electronic payment serves an important evidentiary purpose. In any action involving a consumer, such documentation may be used as evidence of an electronic funds transfer to another person.

A bank customer should immediately upon discovery of an error give notice to the bank whether in writing or verbally. This will facilitate speedy resolution or putting into place of corrective mechanisms.

## 4. AUTHORIZED AND UNAUTHORIZED TRANSFERS

It is important to understand the essential difference from a legal angle between a document and an automatic data transfer. The ordinary payment document, for example, a cheque, retains its identity: a signature on the document will remain there, whether made by an unauthorized person or not – and even if it is forged. Corrections and additions will show on the document itself. Automated data transfer, on the other hand, by its very nature, has a completely different characteristic. Once fed into the computer the data seems to loose its identity; it is retained in a computer memory and becomes accessible only by computer programs. Here also there is a legal aspect. The problem of regulatory law.

Paper borne data is acceptable–but with a known specified legal format, data content and method of authentication. A corresponding legal acceptability of data produced automatically or electronically may not exist. A major problem relating to the computerized data thus is the acceptability of computer records as evidence of payment instruction.

In reality 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.

An electronic funds transfer is commonly initiated by means of an "access device" such as a debit card, issued to the consumer by the financial institution, which is capable of accessing the account from which the customer is permitted to withdraw. Where the use of that access device is by the consumer to whom it was issued, or by another person acting under the consumer's authority, the ensuing electronic funds transfer is authorized. Liability of the consumer to whom the access device was issued for "authorized" transfers emerges from the general principles of Law and is normally backed by the agreement between him and the financial institution.

What is an access device? It is defined as a card, code or other means of access to a consumer's account or any combination, thereof, 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 magnetic tape or other devices used internally by financial institutions to initiate the electronic funds transfer.

The convenience of electronic banking is apparent but so are the risks and subsequent loss brought to bear on the bank's customer should his card be accessed without his consent by a third party who fraudulently gains access to the funds in the bank account for the ATM card holder. Every so often in Kenya, the media reports incidents of the ATM cardholder being forced by thieves to withdraw funds from their accounts through a public access terminal. The Kenya ATM cardholder unlike his United States counterpart is made to be liable and his account debited by the amount of withdrawals at such circumstances. It is important that this issue is addressed by the 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.

The United States Electronic Funds Transfer Act of 1978 ("EFTA") sets out

a number of specific exemptions prompting a bank to refuse to make an electronic payment.

The specific grounds are:[10]

- That there are insufficient funds in the consumers account.
- That the account is subject to legal process or other encumbrances restricting transfer;
- That such transfer would exceed an established credit limit;
- That an electronic terminal has insufficient funds to complete the transaction;

This is the only exemption peculiar to electronic payments. In paper-based systems, the bank's obligation to the customer's mandate is vitiated by the first three exemptions.

- An act of God or other circumstances beyond its control;
- A technical malfunction known to the customer at the time of the attempted transfer.

Under EFTA, a financial institution that fails to make a transfer without lawful cause may be liable to civil action for damages arising thereunder. Likewise, the financial institution may be liable in a civil action for failure to make a transfer or failure to deposit a transfer of funds to a customer's account. The measure of damage is actual damages proved whenever the institutions failure was not intentional resulting from an error made in good faith notwithstanding the maintenance of procedures reasonably adopted to avoid such error.

It is significant that electronic payment issues remain untested in the courts of Kenya and the United Kingdom. What is of more significance however is that both in the United Kingdom and in Kenya, the primary sources of law governing electronic payment are the law of contract and agency and the customs and usages of banking. In the United States, EFTA was enacted specifically for the regulation of electronic funds transfers. This is the primary governing law and resort to the law of contract and agency and in ordinary banking practices is secondary to statute.

Another thing to bear in mind is that EFTA was enacted for the protection of individual consumer rights and to define the rights, liabilities and obligations of parties to an electronic funds transfer. The Act only regulates banker-customer relationships where the consumer is a natural person.

As stated above, 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 "authorized". A customer to whom an access device is issued by a bank is liable for amounts of all authorized electronic funds.

Section 205.2 (m) of Regulations E[11] defines an unauthorized electronic funds transfer as one initiated by a person other than the customer without actual authority to initiate the transfer and from which the customer receives no benefit.

Accordingly to this definition, an unauthorized transfer consists of:

- An electronic transfer of funds out of a customer's account.
- A fund transfer initiated by a person other than the customer.
- The Person acts without actual authority or initiate the transfer.
- The customer derives or receives no benefit.

The customer's liability for "unauthorized" transfers can be limited and subject to pre-conditions.

An unauthorized electronic transfer does not include;

- an electronic fund transfer initiated by a person who was furnished with the access device by the consumer, namely someone with lawful control of the access device, unless the financial institution is notified of the termination of the transaction authority; a transaction which was initiated with fraudulent intent by the consumer or accomplice;
- or a fund transfer initiated by the bank or its employee. In dealing with liability from electronic funds transfer, as distinction is drawn between authorized and unauthorized transfers.

In *Judd Vs Citibank* [12] a decided case in the USA, the court held that in an action involving a consumer's liability for an electronics funds transfer, the burden of showing that the transfer was "unauthorized" is on the consumer. The consumer must first plead transfer and put forward evidence supporting this.

At that point, the burden of proof shifts to the bank, which must prove that the transfer was "authorized". In order to make its case, it is now for the bank to prove that the transfer was initiated by means of the access device it issued to the consumer. At that point, the burden of proof shifts to consumer alleging the "unauthorized" transfer to prove loss or theft of

the access device.

Notice of loss or theft of the access device given to the consumer by the financial institution is a *prima facie* evidence of loss or theft. The bank may then however put forward evidence refuting the loss or theft. Where it is not proven that an access device issued by the bank to consumer initiated the transfer, a presumption arises as to an "unauthorized" transfer. The bank may, however, submit evidence proving an "unauthorized" transfer.

In another case in the United States, *Porter Vs Citibank* [13] the cardholder complained to his bank that three ATM withdrawals on two separate dates from the same machine dispensed no money to him. In each occurrence, he complained promptly. The bank nevertheless debited his account. Strictly speaking, the issue was not characterization of the transfer authorized or unauthorized but rather the mere existence of the transfer. The broader issue however was the existence of authorized transfers with respect to which the consumer is fully liable.

The witnesses employed in the Branch of the bank, where the machine involved was located, testified that upon examining it on the day after the first of the occurrences they found the account in balance while on the later date there was a cash average of $90. They further testified that cash machines were out of balance once or twice per week but never for a sum in excess of $100. The first withdrawal was for $100 and the other two were each for $200. Characterizing the case as another dispute between man and machine, the court held in favor of the customer, finding that the customer had established through evidence that he did not receive the money. This was supported by the fact that they were dealing with machines, which the bank's witnesses acknowledged were out of balance one or two nights a week although not to the extent involved in this case. The bank's witnesses also stated their beliefs that at times a subsequent machine customer took the money belonging to the prior user of the machine. The Court found the customer plaintiff to be a credible witness who had no record of banking problems although he had used the machine numerous times.

The credibility of witnesses and balance of probabilities are universal to all litigations. From this perspective, the authorized or unauthorized transfer issue is not a novelty.

But the principles of cheques law – a customer is bound to take reasonable care in executing his payment instruction to his bank to pay to himself or to the account of a third party a certain specified sum against the balance

standing in credit in his account so as not to by his conduct mislead the bank or facilitate fraud- hold true to electronic payment. However, the burden of proof that the customer was negligent in issuing payment instructions or facilitated the unauthorized issuance of the instructions in an electronic payment presents difficulties that the law is yet to come to terms with it. Cheques payments unlike electronic payments have the advantage of having an audit trail; the cheque itself, the cheque stub and the paying in slip. Further cheque book leafs are sequentially numbered. Missing cheques can easily be ascertained. In the case of electronic payments whereas a computer printout shows the processing of a payment message, the customer refutes initiating the payment message. Proving that the customer is in fact the person who issued the payment instructions or that another person did it under the instructions of the cardholder remains a bone of contention.

Machines do not tell tales. Unless the verification of authentic payment message is verified by use of identification marks peculiar to the bank customer, for example, voice recognition, thumb prints, or retina scans, the terminal wall will not identify, for example that Mrs. A as having used Mr. B's Access device to withdraw funds fraudulently. Rather, it will produce evidence that Mr. B's access device was properly used to withdraw funds from Mr. B's account.

The legal issue of the burden of proof is treated differently in the United Kingdom. As it is, the Bank, which wishes to debit the customers account, the normal rule on the burden of proof would be on the bank to prove that the personal identification number was used and the customer authorized its use.[14] This may prove difficult. Most ATM's do not retain any records of the key strokes entered into by the customer. The bank will, thus, not be able to show what the user of the card keyed in. If an ATM is working offline at the time, the bank will be unable to show that the card had not had its personal identification number erased and a new one encoded in it. Consequently, in the United Kingdom, a practice has evolved, through the Banking Ombudsman and not the courts, which place as the burden of proving that the machine was not at fault on the bank. If the bank can prove that there was no technical breakdown, the burden of proof shifts to the customer to prove definitely that she did not use his card and personal identification number and that a third party gained access to the card and or the Personal Identification Number.

It is not surprising that in the overwhelming majority of cases, the customer is unable to discharge this heavy burden of proof.[15] The lack of a legislative enactment that outlines the rights, liabilities, and obligations of the parties

to an electronic payment agreement unlike the case in the United States bears heavily on English and Kenyan bank account customers. For instance, although the normal rule is that the burden of proof is on the bank, the express contractual terms of the contract between the card issuing and its customers will usually reverse the burden. Many banks provide in their standard terms and conditions that the customer is to be liable for all use made of the card or Personal Identification Number, whether authorized by the customer or not. Such a term allows the bank to debit its customers account even if its no mandate to do so.

In yet another decided case in the United States, *Ognibene Vs Citibank* [16], a rogue who was standing near the bank's terminals memorized the personal identification number of a cardholder who was using a machine. The rogue, who pretended to be engaged in the servicing of the terminals used an adjacent telephone to conduct a fictitious telephone conversation with his employees, after which he asked the cardholder to let him have the use of his card to ensure the terminal was in order. After withdrawing the money by keying in the number, the rogue returned the cardholder saying all was well. The cardholder contested the banks right to debit his account with the amount withdrawn by the rogue, claiming that the bank had failed to introduce a safe method for the use of a card.

The Court held that the bank had been negligent in not taking measures to combat a fraud, which it had been aware and that the bank ought to have provided the cardholder with information sufficient to inform him of the danger when it was confronted by the rogue.

In the United States, a consumer's liability for unauthorized electronic transfer ends with notification to the financial institution that an unauthorized electronic fund has occurred. In *Krusser vs Bank of America* [17] a cardholder believing that his debit card had been destroyed in 1986 failed to notify and advise his bank of a 20 dollar unauthorized ATM withdrawal which appeared in December 1986 statement.

In September 1987, the cardholder received bank statements for July and August 1987, which reflected 47 unauthorized ATM withdrawals with the card, totaling 9, 020 dollars.

The cardholder then notified the bank promptly of all unauthorized withdrawals including that, which appeared in the much earlier statement of December. The Court held that the cardholder's failure to report the unauthorized $20 withdrawal, which appeared on December 1986

statement, barred him from recovering the loss incurred in July and August 1987.

An "unauthorized" 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 USA ensuing electronic funds transfer is nevertheless unauthorized. Consumer negligence under the EFTA and Regulation does not alter the liability for unauthorized transfers.[18]

EFTA is a consumer protection law. The Rights, liabilities and 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 protection accorded by EFTA is wide. Of huge importance is the fact that consumer negligence in use of electronic banking facilities extended to him the by the bank render any subsequent transaction arising thereunder authorized. The transfer, notwithstanding the conduct of the customer, is regarded under the act as unauthorized and for the simple reason of the third party being in unlawful control of the access device at the time of transaction.

On the contrary, the English and Kenyan courts will follow the principles of banking law, and particularly analogy to cheques law. A customer has a duty to take reasonable care when executing his payment message so as not to mislead the bank or facilitate authorized transaction. The customer on breach of his duty is estopped from claiming that a subsequent payment arising due to his negligence is unauthorized and thus restraining the bank from debiting his account.

The issues revolving around the phantom withdrawals remains untested in the courts of Kenya. There is no second guessing how the High Court of Kenya would address the evidentiary issues of electronic evidence, that is, electronic records, processes or printouts and digital signatures. Clearly, the Kenyan court, side by side with the American Court will be disadvantaged. Whereas the American Court would seek judicial resort to the Laws enacted in the country governing specific aspects of electronic commerce competent with an ever growing resource of case law, the Kenyan Court will undoubtedly be groping in the dark and may have to resort to the more advanced body of Law of the United Kingdom. Advancements in

Law in this context refer to regular review and amendment of existing law to fit the existing social, economic, and political environment.

## 5. E-BANKING IN KENYA – A LEGAL VACUUM

There are no specific laws governing the electronic commerce or electronic payments in Kenya. The applicable banking laws are antiquated, however, the banking sector pays no heed to this legislative vacuum. The banking system, albeit later than its European and American counterparts has embraced technology, both information systems and information technology. The players in the banking sector remain aware of the vacuum in the law. However, the exigencies of electronic banking, efficiency, effectiveness, economics far outweigh to the banks the risk of falling foul of the current legal structure of banking business, especially where the banking structure is ill defined (the so called grey areas).

There is no doubt that information technology is both a strategic and a turnaround activity for the banking sector. Banks that were slow on their feet in embracing this technology have found a large chunk of their market niche grabbed from under their feet by banks that revamped their information systems and information technology capabilities and are offering fast and better services coupled with a wide variety of banking products. The banking sector can only shrug at the lack of law governing electronic banking in Kenya. It is not their place to enact laws or weep at the lack of any regulations. All the grey areas in the relationship between bank and customer in respect to electronic bank transfer are governed by clausal terms and conditions that will exempt the bank from liability from any fraud, error or malfunctions in the electronic payment systems.

The use of the contract to limit the liability of the banks is restricted in the United Kingdom and in the USA. In Kenya, existing banking laws and in particular the areas of cheque law have reached their limits of flexibility and the time has come for such laws to be updated to the age of widespread electronic banking. This does not mean that a fundamental overhaul of banking laws is needed, and instead discreet changes are required to address only the specific issues presented by electronic banking and therefore to put it on an equal plane with traditional banking.

### Endnotes

1 Chapter 488 Law of Kenya
2 *Randall Vs City Bank,* 446 NYS 2d 845 (CIV.ct.1981)
3 Carvallo De Freitus, "Virtual Banking and consumer protection, 2000 International Bar Association 2000 Conference, p5

4 (1921) 3 KB 110
5 Mark Harpgood, ED, *Pagets Law of Banking*, 11th Ed, p264
6 Ibid, p265
7 Mcstephan Le Goueff, "The Draft E-Commerce Law, in search of confidence."
8 Vincenzo Sinisi "Digital Signature Legislation in Europe: Virtual Banking and Electronic Payment," Sept 200, International Bar Association 2000 conference, The Netherlands, p12
9 Alan Urbach & John Storck "Alternatively, Electronic Technology and the law," the 1984 Computer Law Symposium, conference Transports 21st and 22nd May 1984, London, p173
10 Section 205.2 (a) (i) of Regulation E, cited in Benjamin Geva, *The Law of Electronic Funds Transfer*, Dec 2000, Lexis Publishing, New York, P78
11 12 C.F.R pt 205 (1996): Regulation E is part of EFTA. It was enacted to enforce the provisions of the latter Act.
12 435 NYS 2d (1980) cited in Ellinger, and Lomneka, *Modern Banking Law*, 1994, 2nd Ed, OVP. New York, p75
13 472 NYS 2d 582 (CIV. CT 1984)
14 Mark Harpgood, Ed, *Pagets Law of Banking*, 11th Ed, 316
15 Ibid, p316
16 446 NYS 2d 845 (CIV.Ct.1981)
17 Cal Rpts. 463 (CIV.ct.App.1994), cited in Geva, p105
18 12 CFR pt 205 (1996)