ELECTRONIC FUNDS TRANSFER: LEGAL IMPLICATIONS AND the LAW IN KENYA

NAME KUTWA ARIBA CHARLES

G34/1123/97

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE (LLB) DEGREE PROGRAMME UNIVERSITY OF NAIROBI.

JULY 2001

DEDICATION

This work is offered as an attribute to my parents Mr & Mrs. Kutwa for their love, affection, support and encouragement without whom I would not have scaled to such heights

To my late Grandfather Mr Amutete for insisting that I should start schooling at a tender age. Thanks Grandpa.

ACKNOWLEDGEMENT

I owe a special debt to my supervisor for this dissertation, MR E M NDERITU , for introducing me to scholastic writing. Mr Nderitu's criticism and advice helped transform my rather simplistic presentation into a concrete piece of work.

I must also thank Mr. Meshack J Onyango (Deputy Director Banking Department) and Mrs. Machoka (Legal Officer) Central Bank of Kenya, for providing me with useful 'field practice' in the interviews I conducted with them.

I wish to extend my gratitude to Rispah, Mr Charles and Ritah for their excellent typing of the original manuscript of this work.

Finally to all my friends in Parklands Kabochi, Kaliech, Brian, Noreen, Mum, Thogo, Kisaka,Elvis, Alex and the entire law class of 2001. You guys provided what lecturers could not provide at law school.

Always..... I will love you!

DOCUMENTS AND MATERIALS USED

(a) Books and articles

1 ELLINGER E A "MODERN BANKING LAW" (1994) Oxford

2 MCLAUNGHLIN and COTEN, "ELECTRONIC TRANSFER OF FUNDS" (1991) 203 NYL30

3 KIRKMAN P "ELECTRONIC FUNDS TRANSFER SYSTEMS," Blackwell (1987)

STATUTES

- Central Bank Act
- Banking Act
- Electronic Funds Transfer Act of USA
- Uniform Commercial Code for USA
- Evidence Act
- The UNICITRAL model law on international Credit Transfers

TABLE OF CONTENTS

CHAPTER FOUR

REGULATION OF EFT's IN OTHER COUNTRIES: A COMPARATIVE STUDY

4.0 The European Community

4.1 U.S.A.

4.2 Australia

4.3 UNCITRAL

CHAPTER FIVE

5.0 RECOMMENDATIONS

5.1 Proposed framework for a new law

5.2 Banking services Act

5.3 The Central Bank of Kenya Act

5.4 The Evidence Act

5.5 A code of conduct

INTRODUCTION

Today's Banker-customer relations belong to quite a different age. International and Local Trade in Kenya now require a banking system that enables quick and efficient transfers of money from one area to another. Due to its efficiency and quickness electronic banking is now recognized as the new dynamics for change in the Banking sector. Electronic Banking lessens congestion in banking halls and also improves customer care. Due to its novelty in our jurisdiction the existing laws and practice seems inadequate in regulating legal problems that have arisen.

Payment by electronic funds transfer has be described as the 3rd of the three great ages of payment. 1st is cash 2nd paper based i.e. cheques, and bills of exchange. There is however no universally accepted legal definition of Electronic Funds Transfer. For the purposes of this paper I will take the United Nations Commission on International Trade law (UNICITRAL)definition. Which is "A funds transfer in which one or more of the steps in the process that were previously done by paper-based techniques are now done by electronic techniques".

There are two categories of Electronic Funds Transfer systems: Non-consumer activated systems and consumer activated systems. In the case of Non-consumer activated EFT system its the Bank which normally selects and activates the system. This include the services operated by BACs Ltd., clearing House Automated Payments Systems (CHAPS), Society for Worldwide Inter-bank Telecommunications (SWIFT), Cheque Truncation and Office Banking. In the case of consumer activated EFT system, its the consumer who selects and activates the particular EFT system to be used in the transaction. Consumer – activated EFT systems include cash dispensers, Automated teller machines, Tele-shopping, digital cash and home banking.

The current banking legislation in Kenya does not address issues in relation to EFTs. Such problems include the authentication of customers or institution instructions, operational security of the system and confidentiality of information that may be collected through the systems, liability for losses due to fraud and technical failure and the regulation of countermand or reversal of instructions. The EFTs having been used in many

jurisdictions and thus have been made subject to legal requirements and regulations in those jurisdictions. These laws can influence the current Kenyan system in a number of ways.

STATEMENT OF THE PROBLEM

It clearly emerges that Electronic Funds transfers are ostensibly meant to enable a quick and efficient transfer of money from one area to another.

However, notwithstanding this fact, it still remains difficult to define EFTs orders i.e. payment instructions and related messages. Moreover, this transfer entails various types of legal transactions. This has led to various problems that are intrinsic to the nature of electronic Funds Transfer.

This research will endeavor to look at the legal implications and problems posed by this mode of funds transfer and the way to solve them and in recommendations and conclusion, it seeks to provide the way forward for Kenya. The legal problems to be looked into are:

1 AUTHENTICATION OF INSTRUCTIONS

Under the paper based systems of payment authentication of the transaction is through signing while in EFTs the authentication is by electronic key whereby a credit transfer is a 'push' of funds by the payee from the payer. This involves the adjustment of the balances of the payee's account and the payer's account.

Another problem is that it is difficult to place the burden of proof especially where there is alleged fraud or error. The customer may allege that he did not use or authorize the use of his PIN (or card) to withdraw or transfer funds. This issue is especially relevant in the case of so called 'phantom withdrawals'.

Another issues, which arise, is the standard of security to be applied and the kind of encryption technology to be used.

2 OPERATIONAL SECURITY OF EFT SYSTEM

These messages on the magnetic material may be altered or erased easily, this becomes complex given that there is lack of written records in case of this system.

3 LIABILITY FOR LOSS IN CASE OF TECHNICAL FAILURE

Its common practice for banks to provide that it shall not be liable for failure to carry out a transaction in the event of mechanical failure of equipment of transmission problems. The thing is the Bank is to bear full loss caused by technical fault in the machines or other systems used, unless the fault was obvious or advised by a message or notice on display. However, the Banks liability is expressly limited to direct loss, which appears to exclude liability for consequential loss. There is need for a legislation to enable an individual customer to recover for foreseeable losses caused by equipment failure despite any clause restricting the banks liability as is the case with paper based system.

4 COUNTERMAND

It is difficult to determine the point at which instructions can be countermanded in EFTs than on paper-based system i.e. in ATMs its not possible to countermand the customers instructions once entered into the ATM. The question that arises is at what time may the instructions be reversed.

5 CONFIDENTIALITY AND DATA PROTECTION

The use of computer technology by Banks and other EFT system providers facilitates the collection, storage and dissemination of customer information. At common law the Bank owes its customer a contractual duty of confidentiality. However as this duty arises only when the relationship of Banker and Customer is established, it would not extend to information acquired by an EFT system provider although they may acquire the information in circumstances which give rise to an equitable duty of confidentiality.

There is no unitary law to EFT between states. The closest model law that has been agreed upon as a compromise legal instrument is the UNICITRALS model law on EFTs.

Kenya has not made specific legislation to regulate EFTs. The question is whether the solving of the above problems can continue to be left to contractual arrangement or whether there is need for a wider regulation in some form.

OBJECTIVES

1 Investigate the current Kenya legal position on EFT system and its regulation and establish the relevance of such legal regulation.

2 Compare system in foreign jurisdiction with current Kenyan system.

3 Inquire into the possibility of introducing UNICITRALS model law on EFTs into the Kenyan legal system.

JUSTIFICATION

1 EFT has become a fast growing sector of the banking industry in Kenya and has shown recent popularity, due to its efficiency, improved customer care and less expenditure involved.

2 EFT system has become important in Kenya in the recent years due to liberation of Kenyan market under the new world order of global trend. The reason for such growth is due to the increase in the flow of funds in and out of the country.

3 EFT system has not been addressed by existing banking laws. The existing law in Kenya has not been updated to deal with the new banking service and the problems that may arise from these transaction.

HYPOTHESIS

1 Due to globalization of trade in the world of Kenya the EFT has marked increase in Kenya in recent years.

2 Due to increase in EFT transactions there is need to have a Kenyan legislation regulating the EFT system.

3UNICITRALS models law on EFT system should be adopted into Kenyan system to regulate its transaction in our jurisdiction.

RESEARCH METHODOLOGY

1 Personal interviews with professionals and people involved in the Banking sector i.e. legal officers, Central Bank officials etc.

2 Personal collections.

3 Library research (British Council UN library and Central Bank records)

4 Newsweek magazines, Business Weekly magazine.

5 Internet (Websites)

CHAPTER ONE

1 HISTORICAL DEVELOPMENT OF PAPER BASED SYSTEMS TO THE PRESENT DAY EFTS

There are two paper-based systems of payment, namely the bills of exchange and the cheque. The latter simply refers to the former. Ancient bills of exchange owe their history to the business practices obtaining particularly after the fall of the Roman Empire, when the Arabs became the main players in western commercial world. They were later replaced by the Lombard who were Italian merchants from Genoa, Liucca, Florence, and Venice.[1]

The trade merchant, bankers and moneychangers had agents and correspondents in many different countries, an incidence of their constant journeying from country to country. It became necessary to design a way in which money could be transferred from one country to another without the risk attached to carrying it in specie.[2]

Although it may not be possible to state the exact year when ancient bills of exchange (or at least their analogy) came into use it may suffice to pinpoint the undisputed observation made by **Hold worth** that[3]

> "It is certain that in the eighth century AD long before anything like the bill of exchange appeared in Italy, something very much like the modern bill of exchange was known. It could pass from hand to hand by something very much like an endorsement; and to use modern terms, the payee had a right of resource against the drawer in the event of non-payment of the acceptor."

The Bill of Exchange was introduced in England as early as the thirteenth century and by the mid of the fifteenth century it was prevalently used among the Italians and their clients. It took the form of a commercial paper.[4]

The cheque was and is the most demanded for paper based system of payment. The cheque system originated with the goldsmiths. For various reasons merchants began

---

[1] HOLDEN J. M "the history of negotiable instruments" london, 1995 pg. 1

[2] N. T BAXTER", credit bills book-keeping in a simple economy, the accounting review; london, 1946 pg. 154 - 166

[3] HOLDSWORTH, SIR W.S, history of English law, pg. 133

to leave their money in the hands of the goldsmiths and to receive interest upon those sums. Moreover, they soon looked to the goldsmiths to assist them in making payments to third parties. **Holden**[5] postulates that the mode of payment was effected by addressing a short letter to the goldsmith requesting and authorizing payment of the sum due to the merchants' creditor. The creditor would take this authority to the goldsmith's 'shop' and there receive the sum in specie. This was the origin of the cheque system.

The use of cheques for payment of debts was not solely restricted to merchants. Banks indebted to each other could settle their accounts by means of cheques. With this originated the clearing system and the establishment of London clearing house. The establishment of a common clearinghouse positively transformed this onerous and time-consuming task. The underlying principle remained unchanged and to a large extent remains in Kenya.

Today's **EFTS** traces its roots back to 1918 when federal banks first moved currency (i.e. manipulated book - entries to clear payment balances among themselves) via telegraph. However, the widespread use of electronic banking did not begin until the automated clearinghouse was set up by the US federal Reserve in 1972. Similar systems emerged in Europe around the same time, so electronic banking has been widely used throughout the world on an institutional level for more than three decades.

Although banks have been able to move currency electronically for decades. Only recently has the average consumer had the capability to use electronic transfers in any meaningful way.

1.1 GENERAL DISCUSSION OF ELECTRONIC FUNDS TRANSFERS

In local (domestic) or international credit transfers, each payment order, whether between the payer and his bank or the banks themselves, can be given orally, in writing, or by electronic means. In the past, payment orders were communicated between such banks by airmail, by telegram or by telex. However, most banks now communicate with

---

[4] Holden op. at pg.21
[5] HOLDEN op.

their counterparts using the telecommunication network operated by the society for Worldwide Inter-bank Financial Telecommunication (SWIFT).[6]

SWIFT was founded in 1973 by 239 European and North American Banks in the form of a non-profit making society under the Belgian law with headquarters in Brussels. SWIFT became operational in May of 1977. Since then it has grown considerably. There are now over 3,900 banks connected to the SWIFT system and it operates in over 100 countries. SWIFT operates a network of communications, which can be used by banks and other financial institutions for money transfers, opening letters of credit, and generally for transmission, of messages from institution to institution. Its primary objective is to provide a network for members to pass rapid instructions relating to financial transactions between each other.[7] Receipt of a SWIFT message does not in itself constitute a payment transaction; no funds strictly flow through the system and there is no settlement in SWIFT. Nevertheless, a message can still constitute a valid instruction to make a payment and therefore create a mandate with whose terms a bank must comply.

The current SWIFT system is SWIFT II, which came into operation in 1990. Individual banks have access to the SWIFT system through regional SWIFT access points (SAPs'). Each country is assigned to a SAP: the UK's SAP is located at BACs' headquarters in Edgware. SWIFT 2 now comprises a number of slices each of, which is effectively a network that receives a message. Forwards them, and stores them. Each slice is composed of modular elements capable of functioning independently and a slice processor carries out its operations.

When a customer instructs his local bank e.g. Barclays Bank to carry out a monetary transfer under the SWIFT system the bank terminal to the regional or National SAP conveys his instructions. This can be done by a special SWIFT link or by means of a telex message. The SAP encodes the message and dispatches it to the slice processor.

---

[6] Alternative providers of telecommunications Networks include, GE information services and Financial Networks Association.

[7] E U Byler and J.L Baker "SWIFT: A fast method to facilitate Financial Transactions."(1990) 17J world Trade. 458

This message has to set out all the relevant details concerning the transfer in order to complete the transaction. The slice processor transmits the message, after verifying some encoded security numbers, the message is decoded and transmitted to the recipient bank. It completes the transaction by using the facilities available for domestic transfers.

SWIFT transfers are available for twenty-four hours a day and are expected to reach their destination on the same day. Messages are stored at the SAP if they arrive after it has closed for the day. They are processed on the next day in the order in which they were received, except priority messages, which are put at the head of the queue.[8] At the present, there is a growing conviction in the banking sector in Kenya that the safest and fastest way to effect money transfers is by means of SWIFT. The popularity of this system thus has increased in Kenya.

Since the 1990s, the global aspect of banking in Kenya has become much more apparent and in its own respect, due to the liberalization of the Kenyan market and the new aspect of banking available through new technology. This has also rendered possible new types of banking transactions to and from the Kenyan jurisdiction. The spread of electronic banking is as a result of the deregulation of the domestic market in response to the New World order of free market trade.

Electronic banking services have been seen as a marked acceleration in growth in comparison to the expansion of the cheque usage. As banking becomes more computerized and computers grow more sophisticated, electronic impulses are increasingly being used for an ever wider range of bank to bank telecommunications, with a consequent spreading up to transactions in many areas of banking business. With the first generation electronic banking technology, for cheque clearing and computerizing of accounts now well established, we are seeing a major development of second-generation technology. This technology includes the use of shared ATMs, introduction of real-time gross settlement

[8] Electronic Banking - The legal implications", Edited by Goode, R. M (1985) Queen Mary college, university of London.

(RTGS) and Electronic Funds transfer at point of sales (EFTPOs) which are all supposed to herald a cashless shopping revolution.[9]

Recently, in Kenya in line with these developments, home and office banking systems, internet banking and international Electronic funds transfers have been introduced as part of the new banking generation. Such improvements have in general given customers increased convenience and flexibility but have come with new legal problems to the banking sector.

1.2 DEFINITION AND NATURE OF EFTs

Kenya has not been exempted from these legal problems. The introduction of this study, described Electronic Banking as the new dynamic for change in the Banking sector, with its rather novel crop of legal problems that existing law and practice seems most inadequate. Since the introduction of EFTs the greatest problem that was faced was the proper definition of an EFT transaction. Various definitions, judicial, statutory and scholarly have been offered in various works. Each type of definition has tried in essence to capture all aspects related to an EFT transaction from point of initiation to the point of implementation. While most of this definition have tried to create a perfect legal picture of this transaction most have fallen short of this goal.

Webster J in ROYAL PRODUCTS LTD V. MIDLAND BANK LTD[10] held the view that EFTs involve a string of operations carried out by the different banks acting in a representative capacity. He stated that EFT transfers, "

> 'Are to be regarded simply as an authority and instructions, from a customer to its bank, to transfer an amount standing to the credit of its account with another bank being impliedly authorized by the customer to accept that credit by virtue of the fact that the customer has current account with it, no consent to the receipt of the credit being expected from or required of the bank, by virtue of the same fact. It is in other words, a banking operation of a kind which is often carried out internally, that is to

[9] barclays bank plc v.quincare ltd

[10] (1981) & lloyds rep. 194

stay, within the same systems of one bank and which at least from the point of view of the customer, is no different in nature or quality when as in the present case it is carried out between different banks."

The banker's duty of care in the light of the above statement could be said to be supplemented by a more general duty of care implied by the common law. **ATKIN L. J** and **BANKES L. J** laid this principle down over seventy years ago when they pronounced that[11]

"I think that it is the duty of the bank, arising out of the contract, to exercise reasonable care and skill in dealing with communications which the customer sends to (him) in relation to his banking business".

The relationship between the parties is contractual and that the principle obligation upon the bank is to honor its customers obligations and there is nothing in such a contract, express or implied that would require a banker to consider the commercial wisdom or otherwise of the particular transaction.[12]

Despite the recent popularity of these transactions and operations, there remains a dearth of case law in point. Most of the case laws definitions have not quite clearly exhausted the divergence of transactions and operations involved in EFT transaction. Various jurisdictions have been forced, due to the popularity of EFT transactions to come up with statutory definitions of the same. In the USA such transactions are defined as;

"Any transfer of funds, other than a transaction originated by cheque, draft or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account. Such terms includes, but is not limited to point of sale transfers, automated teller machines, direct deposits or withdrawal of funds and transfers initiated by telephone."[13]

---

[11] Westminister Bank LTD V. Hilton (1926) 43 TLR 124

[12] BRIGHTMAN J in Karak Rubber Co. V. Burden (1972)ALLER Pg. 1211

[13] USA Electronic Funds Transfer Act of 1978

This definition seeks to consolidate both the technical and legal problems in one comprehensive definition. By doing so this definition clearly states the difference between a paper based system and an electronic based system. It states that the characters of paper based systems and undertakings are that they embody a transaction in permanency form, are typically expressed in words and figures and are authenticated by a signature identifying the party giving the payment message. Finally, the delivery of the message usually takes a significant period of time.

This definition them explains that in an electronic system, the payment message is expressed in computer code, the handwritten signature is replaced by an electronic key designed to authenticate the message. The message on the tape, disk etc may be, in the absence of security measures, be altered, erased, or transferred to other magnetic material without this fact being discovered from an examination of the medium. This definition does not suit Kenya, which has adopted a two tier system of mixing paper based and electronic system of funds transfer.

On 25th of November 1992 the United Nations General Assembly approved the report of the United Nations Commission on International Trade Law (UNCITRAL). This report of the UNICITRAL included a model law on Electronic Funds Transfer,[14] which the General Assembly recommended that all members states should enact legislation based on the model law. This model law has set out to aid legislators and lawyers of developing countries like Kenya where Electronic Banking is a novel idea. The approach followed while writing this legal guide was to first identify forty-one legal issues arising in the use of this banking service.

The first main problem that was presented was a proper, all-round and accepted definition of an EFT transaction. The model law defines such a transaction on a very broad basis as;

> "A funds transfer in which one or more of the steps in the process that were previously done by paper based techniques are now done by electronic techniques."

---

[14] Resolution 47/34 of 1992

This definition covers funds transfers in which electronic techniques are used at some stage of the transaction, even though the transaction itself may have been initiated by a paper based payment instruction. This definition seeks to achieve the greatest possible degree of legal harmonization between different countries and their various legal definitions. While recognizing that there may be no single definition that suits all systems the UNCITRAL definition allows each state whether developed or developing to introduce an EFT service in the light of its previous wholly based paper based systems.

CHAPTER TWO

2 TYPES OF EFT SYSTEMS IN KENYA

"The 21st century will not be 'cashless' as many now predict. However, it does seem clear that the currency of the 21st century will be 'paperless'. Paper currency and cheques are gradually being supplanted by smart cards, digital cash and instant transfer of funds. The large paper bureaucracy of banks is quickly becoming redundant, burdensome, even antiquated. Some sat that the evolution in digital money is happening so fast that banks cannot adopt quickly enough and will eventually collapse like top-heavy giants blown over by the winds of financial change. May be, or may be not, but one trend is already clear. The wallet of the future will hold less paper cash, coins and magnetic stripe cords. It will hold instead smart cards containing digital cash and other financial information updated, perhaps automatically. The question is no longer if this evolution will happen, but when".

GEOFFREY TURK CEO FEDERAL RESERVE BANK CLEVELAND

There are two categories of EFT systems: Non-consumer activated systems and consumer – activated systems.[1] In the case of non-consumer activated EFT system, it is the bank which normally selects and activates the system.[2] Some corporate or institutional customers may be given direct access to these systems, but the banks consumer customers i.e. its personal account holders do not have similar direct access. In most cases the consumer customer will not even know that the bank intends to make the transfer using an EFT system, although in some cases, the customer may instruct the bank to use a particular electronic systems, leaving it to the bank to activate that system. Non-consumer activated EFT systems services operated by clearing house, automated payment system

[1] S SAXBY (ed) ENCYCLOPEDIA OF INFORMATION TECHNOLOGY LAW (1990) Sweet and Maxwell, London Para S.04

[2] This chapter concentrates on those EFT systems used by Banks only.

(CHAPS) otherwise known as automated clearinghouse in Kenya. The system operated by swift, cheque truncation and office banking.[3]

In the case of consumer – activated EFT system, it is the consumer customer who selects and activates the particular EFT to be used in the transaction. Consumer – activated EFT systems include cash-dispensers, automated teller machines, electronic funds transfers at point of sale, Tele-shopping, digital cash and home banking.

2.1 NON- CONSUMER ACTIVATED EFT SYSTEMS

Electronic payment systems have been developed to facilitate the transfer of funds between bank accounts. The transfer process itself is commonly known as a 'fund transfer' and involves the adjustment of the balances of the payer's account (a debit) and the payee's account (a credit) at their respective banks. There are two types of funds transfers: Credit transfers and debits transfers. It will be useful to outline the principles which govern the operation of these two types of funds transfer before examining the mechanics of the various non-consumer activated electronic funds transfer systems themselves.

A credit transfer is a 'push' of funds by the payer to the payee. The payer instructs his bank to debit his account and to cause the account of the payee at the same bank or another to be credited. The payer's instructions may be for an individual credit transfer e.g. the CHAPS payment or for a recurring transfer of funds under a standing order which will be paid using the BACS system.[4] On receipt of the payer's instructions, the payer's bank will debit his account and forward instructions to the payee's bank, which will credit the payee's account.

A debit transfer[5] is a 'pull' of funds by the payee from the payer. The payee conveys instructions to his bank to collect money from the payer. These instructions may be initiated by the payer himself and passed on to the payee e.g. as happens with the collection of cheques; alternatively, they may be initiated by the payee himself pursuant to the payer's authority, as happens with direct debits. On receipt of instructions from the

---

[3] Office banking is a non-consumer from Electronic Banking, but because of its similarities with home banking the two will be considered together.

[4] An automated clearinghouse which provides bank Electronic clearing of transfers.

[5] otherwise known as a 'debit collection'.

payee, the payee's bank will provisionally credit the payee's account with the amount to be collected and forward instructions to the payer's bank, which will debit the payer's account. The credit to the payee's account becomes final when the debit to the payer's account becomes irreversible.

Where the payer and payee have accounts at the same branch of the same bank (known as an intra-branch transfer) or at different branches of the same bank (known as an inter-branch transfer), the same bank will act as both the paying bank and the receiving bank, and the transfer if funds between its customer's accounts will essentially involve an internal accounting exercise at that bank. The position will be different where the payer's account and the payee's are held at different banks (known as an Inter-bank transfer). In inter-bank transfers, the receiving bank must be put in funds by the paying bank. This process is describes as settlement and can occur on either a bilateral or multilateral basis. Bilateral settlement occurs where the paying bank has an account at the receiving bank enabling the receiving bank to debit that account with the amount it has itself credited to the payee's account. Multilateral settlement involves the settlement of accounts of the paying bank and the receiving bank held at a third bank i.e. central bank of Kenya.

2.1.1 REAL-TIME GROSS SETTLEMENT (RTGS)

This system is operated by CHAPS. The system handles settlement transactions between financial institutions operating in the market. Plans are underway to introduce RTGS in Kenya by the end of July of 2001 to facilitate a quick transfer of funds and securities between transacting parties.

Under RTGS system which is used mostly by European countries, each payment message is settled across member's accounts held at the Bank of England, for Kenya. It is the Central Bank of Kenya, as soon as they occur (in real time) and so settlement risk has been significantly reduced.

Under this system each payment message is settled across member's accounts at the Central Bank before it is sent to the receiving bank. If there are sufficient funds in the sending banks account, the Central Bank will settle the transaction by debiting the sending bank's account and crediting the receiving bank's account in the same amount, and then

return a confirmation to the sending bank. On receipt of this confirmation, the payment will be released automatically to the receiving bank by the sending bank's gateway. When the payment message is received by the receiving bank it will immediately transmit a logical acknowledgement message (LAK) back to the sending bank. The receiving bank has assurance that on receipt of the payment message the relevant funds have been credited to its settlement account.

2.1.2 CHEQUE TRUNCATION

Each day up to 100 thousand cheques move around the general cheque clearing system. This is time consuming and a costly process which involves the physical transportation of each cheque from the branch of the collecting bank where it has been deposited by the payee for collection, via the clearing house, to the branch of the paying (drawee) bank in which the cheque is drawn cheque truncation would short-circuit this process instead of the cheque being physically transported from the payee bank to the paying bank. Data from the magnetic ink code line at the bottom of the cheque[6] would be sent electronically from the collecting bank to the paying bank, with the cheque being retained by the collecting bank.

The collecting bank owes a duty to its customer to present for payment all cheques deposited for collection.[7] The act provides that the cheque must be duly presented for payment and that failure to do so discharges the drawer and endorsers. It has to be presented 'at proper place' and 'at reasonable hour on a business day'. However the cases indicate that a cheque must be physically presented for payment and the presentative by electronic means would not comply with the requirements of this act.

2.2 CONSUMERS – ACTIVATED EFT SYSTEMS

2.2.1 Cash Dispensers (CDS) and Automated Teller Machines (ATMs)

The first CDs in the world were introduced in the UK in 1967. A CD is an ATM, which only dispenses cash. ATMs can provide many more services than simply dispensing

[6] Cheques are issued to customers with the bank and branch number the cheque number and account member encoded on them in machine readable form; and when the cheque is deposited for collection the payee's account details and amount of the cheque are also added in machine readable form. The process is called magnetic ink character Recognition.

[7] HARE V HENTY (1861) 10 CBNs 65.

cash. Typically a customer can use an ATM to make a balance inquiry, order a cheque book and order a bank statement. Some ATMs allow the customer to initiate the transfer of funds between his own accounts or to the account of a 3rd party and even to receive deposits into his account.

In order to gain access to an ATM, the banks customer is issued with a plastic card[8] bearing a magnetic stripe together with a four – digit personal identification number (PIN). The customer inserts his plastic card into the machine followed by his PIN. After the Pin has been verified the ATM will display a menu of its functions. The customer selects the menu he requires follows the instructions displayed on the ATM his card is returned to him at the end of the transaction.

2.2.2 Electronic Funds Transfer at Point of Sales (EFTPOS)

EFTPos allows payment to be made for goods and services by the Electronic transfer of funds from the customers account to the suppliers account. In the case of a retail payment instead of a customer paying for goods or services by means of cash or cheque he presents a cashier with a plastic EFTPos debit card, which has information relating to the customers bank account, encoded on a magnetic stripe on the magnetic stripe at the back. The cashier 'swipes' the card through a card reader installed at the retailers point of sale terminal and enters the amount of the transaction.[9] The authorization request, and its subsequent acceptance or rejection will be sent over a telecommunication link via the authorization center of the retailers own bank. Where the card has been accepted the terminal will produce a transaction voucher for the customer to sign. The cashier then compares the customer's signature acts as the customer's mandate to his bank to debit his account and credit the retailers account and a message to his effect is transmitted; via the EFTPos network to the customer's bank and the retailers bank.

2.2.3 Home and Office Banking

The first Home Banking service was introduced in UK by the bank of Scotland in 1982 and since then other major banks and building societies around the world have

---

[8] Sometimes called a 'cash point card' or 'ATM card'

[9] Although credit card transactions may also be executed using ETPOs terminals eg visa and master card operate systems.

followed suit. In fact, Kenya has not been left behind. Home Banking allows a customer to access his account from his own home or office. Typically, it will allow the customer to make balance inquiries, transfers funds between accounts cheques book and statements. The customer accesses his account by means of a computer terminal

2.2.4 Internet Banking

To date, commercial banks in Kenya have shown only limited interest in the internet. Given their focus on private, proprietary networks, it is not surprising that banks view it with misgivings a computer networks, which have been established to facilitate the free exchange of non-sensitive and non-financial information.

CHAPTER THREE.

3 ELECTRONIC FUNDS TRANSFER AND THEIR LEGAL PROBLEMS

Despite the popularity that Electronic Banking has attained in the course of the last 20 years, it has been difficult to define and tackle its legal problems. The divergence of transaction covered under the umbrella of EFTs contrast with the old paper – based systems, whose nature is clearly defined. Legally there are only three points to an EFT transaction that can be said to be clearly defined and agreed upon. The first is that, documents used in EFT transaction are not negotiable instruments. Secondly, the law of assignment is in all probability inapplicable. The third and only positive rule is that for most purposes the relationships of the parties to money transfer orders are governed by the law of agency. While it is clear that the banks involved act in a representative capacity, it is frequently difficult to determine on whose behalf a certain bank is acting for, at a particular moment. This question may be important when determining the point of time at which the payer loses the right to countermand his payment order.

3.0.1 LEGAL NATURE OF A FUNDS TRANSFER INSTRUCTION

The legal nature of an instruction given by the payer to his own bank (paying bank) to transfer funds from his account to the account of the payee, or to another one of his own accounts, held at the same or a different bank, was summarized by **Webster J in Royal Products Ltd. V. Midland Bank Ltd. as follows[1]:-**

> "In my judgement they are to be regarded simply as an authority and instruction, from the customer to its bank, to transfer an amount standing to the credit of that customer with that bank to the credit of its account with another bank that other bank being impliedly authorized by the customer to accept that credit by virtue of the fact that the customer has an own account with it... It is, in other words, a banking operation, of a kind which is often carried out internally, that is to say, within the same bank or between two branches of the same bank and....which is no

[1](1981) 2 Lloyd's Rep 194 at 198

different in nature or quality when as in the present case, it is carried out between different banks[2].

Strictly speaking there is no transfer of funds involved with a funds transfer operation as cash is not transferred from one account to another, and the paying banks original payment obligation owed to the payer is not assigned to the payee. On the contrary what happen with a funds transfer is that the debt owed to the payer by his bank the paying bank, is extinguished or reduced pro tanto by the amount of the 'transfer' to the payee, whilst the debt owed to the payee by his own bank, the receiving bank is increased by the same amount.

3.0.1.1 THE PAYING BANK

Where the payer is a customer of the bank instructed to make the transfer of funds, the primary relationship between the bank and its customers is that of a debtor and a creditor[3]. The bank is under a duty to obey the customers mandate. Where the bank acts outside the mandate for example transmitting a payment message to the wrong bank, to the wrong payee, or in the wrong amount, it cannot debit its customers account[4]. The paying bank is engaged in EFT in a representative capacity. Acting as an agent the Bank owes the customer a duty to observe reasonable care and skill in and about executing the customer's orders.

The paying bank's duty of care and skill imposes on it three specific obligations. The first is that the amount has to be transferred on time. Thus, if a specific time for transfer is expressly specified in order, the bank has to comply with the deadline prescribed if it accepts the instruction to transfer. Usually the time of transfer is discernible from the circumstances of the transaction.

The transferring bank's duty to act promptly and with skill applies not only to the execution of the payer's payment instruction but also to the handling of a stop order issued by him. In the case of **Mellon Bank V. Securities Settlement Corp**[5]. SSC at the request

---

[2] W.J concerned with transfer of funds between accounts held by the same person but same principles apply when the transfer is between accounts held by different persons.
[3] Folley Vs Hill (1848) 2 4 L Cas 28
[4] Urr Vs. Union Bank (1854) 1 Macq 513
[5] 710 .F. Surf 991 (D. New Jersey 1989)

of its client K. Instructed to M. Bank to transfer an amount of US$ 113,080.50 to the account of one B with the F Bank. An appropriate message was dispatched forthwith by the M Bank to the F Bank through the intermediary of the M Banks, MHT. Later SSC discovered that K did not have the means to reimburse it. SSC accordingly instructed the M Bank to stop the payment. MHT was informed accordingly. By the time the error was discovered, B had withdrawn the funds credited to his account by the F Bank. Fisher D J held that the M Bank was not entitled to claim reimbursement of the money paid to B. It owed SSC a duty to exercise care and skill in the execution of the stop order given to it. Thus it breached its contractual duty of care.

The paying bank will be vicariously liable for the negligence or default of its employees and agents. In particular it will be liable for the negligence of any correspondent bank, which it employs[6]. However, it is common practice for the paying bank to disclaim liability for negligence and default of its correspondent. Clauses disclaiming liability are usually set out in standard payment instruction forms supplied by the paying bank for the customer's use.

The paying bank's contractual duty of care and skill does not extend to the payee. However following the approach recently adopted by the house of Lords **in Henderson V. Merret Syndicates Ltd.**[7] It might be possible to establish such a duty of care under the **Hedly Byrne Principle**[8]. Which was explained in terms of assumption of responsibility by the defendant. It could be argued that the paying bank's assumption of responsibility to its owns customer, the payer should be extended to the intended beneficiary of the payment, the payee, if so this would create a new category of special relationship to which the law attaches a duty of care to prevent economic loss.

3.0.1.2 THE RECEIVING BANK

The receiving bank also acts in a representative capacity. It receives the payment instruction from the paying bank, or (via its correspondent if its an internationals funds

---

[6] Equitable Trust Co. of New York Vs. Dowson pathers Ltd. (1927) 27 Ll. LR 49
[7] (1995) 2A . C. 145
[8] Hedley Byrne 8 Co. ltd Vs Heller 8 patners ltd (1964) AC 465

transfer) as the paying banks agent, but once the receiving bank executes the instruction or otherwise accepts it, the bank does so as the payee's agent, provided it has payee's actual or ostensible authority to do so. However, the agency relationship will only be momentary as the receiving bank immediately borrows the money representing the transferred funds back from the payee and the underlying debtor – creditor relationship of bank and customer is restored.

The receiving bank owes its customer, the payee a contractual duty of care and skill. The duty mirrors that owed by the paying bank to the payer. The duty extends to the way the bank process a payment received from the paying bank, but also means that the bank should exercise a reasonable care and skill to maintain its equipment in a condition that it can receive the payment in the first place. The bank may also be under a duty to advice the payee that payment has been effected.

3.1 LEGAL ISSUES ARISING FROM EFT

Having outlined, above, a general approach of EFT regulation it would be proper for me to turn to more specific problem areas. These areas include Authentication of a customer's instruction; operational security on existing systems; liability in case of loss due to fraud or technical failure, confidentiality and Data protection; and countermand and time of payment.

3.1.1 AUTHENTICATION OF INSTRUCTIONS

Under the general law of contracts, the authentication of customer's instructions is required in all payment modes. However in the case of EFT no satisfactory technique has yet been evolved, which enables those instructions to be personalized in the way paper-based debit transfer instructions have been personalized by the customer's signature on a cheque. Magnetic material shares with paper based items the characteristic that the transfer medium is tangible and movable, so that the messages stored on it can not only be located but can be recalled prior to their delivery to the intended recipient. There, however, the resemblance ends. The payment message is expressed in computer code, the handwritten signature is replaced by an electronic key designed to authenticate the message. In the absence of security measures, the message on tape or disc may be

altered, erased or transferred to other magnetic material without the fact being discovered from the examination of the medium.

Any system that requires keyboard input to validate a transaction is open to fraud. This was expressed in an EC report[9] which contends that levels of security are inadequate. Secondly that user authentication methods are proving inadequate. Thirdly in complex networks system security has often had a low priority because cost – effectiveness has been wrongfully assessed. Fourth and lastly that a radical alternative is needed to existing technology.

At present the four (4) digit authorization procedure known as the **PIN**[10] is in use nationally and internationally. The validity of **PIN** authorization has not been tested or subjected to serious judicial scrutiny in courts of this country nor are Banks pushing for it to be given statutory recognition although it has been accorded that in some countries. The **PIN** is supposed to be memorized and not recognizably written down in a place where others have access to it. It can only be activated if both the correct card and the correct **PIN** is noted by watching it when keyed in and a card is stolen, it is relatively easy to forge cards by wiping out the existing information in the magnetic strip and inserting new data.

There is need for banks to introduce **on-line** cards. The danger of **off-line** is that it has no direct link, for individual transactions, with the central computer of the bank. The person who misappropriates the card may succeed in decoding the **PIN**. In contrast, an **on-line** card does not have any record of the **PIN**. Instead, the number is retained by the central computer, to which the terminal is linked (or on-line) the danger of abuse is minimal. Unfortunately, many holders who find it difficult to remember their **PIN**, carry a record with them. If this falls into the hands of a thief together with the card itself, misuse becomes easy. Liability for misuse has to be considered in light of common law principles.

The common law approach is best illustrated by an American authority, **Judd V. Citibank**[11]. The cardholder disputed the debiting of her account with an amount of $800, which was shown on her statement as having been withdrawn by the use of cash point

---

[9] Security or networks system's coppers and Lybrand DG XIII European Commission (1998)
[10] PIN
[11] 435 NYS 2d 210 (1980)

card. The **ATM**[12] machine involved was programmed to effect a withdrawal only if the card was verified and the numbers on it were matched with the **PIN** keyed in. She testified that at the time of withdrawal she had been at work and she had not entrusted her card to anybody and that she had kept her **PIN** to herself. The New York court gave judgement for the cardholder. The relevant issue was identified as follows:-[13]

> "has (card holder)she proven her case by fair preponderance of the credible evidence? In this case we are met with a credible witness on the one hand and a computer printout on the other."

The court took into consideration that machines were subject to breakdowns and concluded:

> "This court is not prepared to go so far as to rule that where a credible witness is faced with the adverse 'testimony" of a machine, he is a matter of law faced also with an unmet burden of proof. It is too common place in our society that when faced with the choice of a man or machine we readily accept the 'word' of the machine every-time,. This, despite the tales of computer malfunctions that we hear daily."

An English court, faced with a similar problem, would have to consider an additional point. The master agreement between the bank and the cardholder includes a clause under which the bank's record is deemed conclusive proof of transactions effected through the use of Teller machines. Clauses of this type have been held in the context of performance bonds and first demand guarantees, where the term usually states that a demand made by the beneficiary of the facility constitutes conclusive proof of the happening of the event on which payment is due. There is however a difference between the object of a conclusive evidence clause in a performance bond agreement and the comparable clause in a point card agreement. In the former case, the object of the clause is to enable the bank to honor its undertaking without getting embroiled in disputes between the beneficiary of the performance bond and the 'account party' at whose request the

---

[12] ATM
[13] Ibid. 211

facility was furnished. In the other case the object of the clause is to preclude the banks customer - the cardholder – from disputing inaccuracies in his statement.

As to available alternatives, one is electronic signature recognition, which was introduced recently in Kenya. It allows a customer to activate EFT system simply by signing his name. The technology is based on recognition of the impulses that underlies a signature, rather than appearance of the signature. The other alternative could be a form of Biometrics identification technique such as fingerprints, palm print or voice recognition. Apart from technical and cost problems associated with these techniques, these solutions may not find social acceptability.

It is therefore clear from the above discussion that an **EFT** system must meet certain minimum standards of security in its authorization procedures to provide acceptable degree of protection for the customers against the consequences of unauthorized instructions. Banks should ensure that privacy is provided to a customer when he is keying in his **PIN** to make it physically impossible for a customer **PIN** to be read by anybody else, when it is being keyed in.

3.1.2 OPERATION SECURITY STANDARDS

Computers have raised a new problem of security in that unauthorized persons can easily gain access to the computer network and confidential information therein. Thus the legal protection of the customers finances with the bank is rendered illusory. The fact that it is difficult to monitor the transfer of information using computers has raised new controversies over rights of privacy.

Computer networks are essentially public in their scope of operation because the information transmitted over them can be assessed anywhere between the points of origination and destination. Even private computer networks are not immune to wiretapping and surveillance by determined infiltrators. The science of cryptography, which is the science of keeping digital data secure, makes this possible. Encryption is the process of scrambling data into ciphers or code so that it can only be unscrambled

(decrypted) by individuals who have the key essential to accomplish this task[14] suffice is to say there is strong encryption and weak encryption.

Computer – based encryption using PCs is, in principle capable of becoming sufficiently secure to prevent unauthorized access. However, the ability to encrypt messages, is presently restricted by the requirements of nation states to have access to all written communications, a right that was in the past enshrined in controls placed on postal, telegraph and telephone services. This limits efficacy of encryption giving it a role similar to fitting window locks as a means to prevent burglary. Still, a number of software companies are presently developing encryption software. Some of which are based on patented algorithms[15].

Monitoring suspicious patterns of ATM withdrawals could be one of the modes of ensuring operational security. If banks run a computerized system, which automatically flags a suspicion pattern of withdrawals at an early stage, further action can be left to the managers discretion, which in some cases call for difficult and delicate judgement. This solution could at best be termed fraud preventive[16].

Written records should be a standard contractual requirement. Both US EFT Act and Australian code of good practice make a standard requirement of documentation for all customer activated **EFT** and prescribe in detail what information they should provide. In return, a customer should be entitled to demand a written record of an **EFT** transaction if he wishes to have it.[17]

3.1.3 LIABILITY IN CASES OF FRAUD OR TECHNICAL FAILURE

Lapses in security and technical failure of EFT equipment raises serious questions of apportionment of liability. In case of any direct, or clearly consequential loss due to failure of an **EFT** equipment to complete a transaction, the bank should normally be held

---

[14] Money and currency in the 21 century (GEOFFREY TURK) JULY 1997
[15] Economist

[16] Legal issues arising out of technologically advanced payment systems. NV. DESH PANDE. Article published in the journal of the Indian Institute of Bankers Vol. 66/No.4 Oct – Dec 1995
[17] Ibid at 147

liable to the customer. Apparently it has become common practice for the card issuing Banks and those who offer **EFT** services to provide that it shall not be liable for failure to carry out a transaction in the event of mechanical failure of equipment or transmission problems or where the circumstances beyond the banks control prevent the transaction from being effected[18]

Banks incorporate terms and conditions in the contract which exclude liability on part of the bank. It is high time bank's shouldered the full loss caused by technical fault in the machines or other systems used, unless the fault is obvious or advised by a message or notice in the display.

In case of fraud a customer in any customer – activated **EFT** system should normally be held liable for any losses incurred up to the point, where he notifies his bank. In cases of fraud an issue arises as to whether the customer can institute an action against the receiving bank to recover money wrongfully paid from his account. Until recently the prevailing view was that a customer could not institute an action to recover money wrongfully paid, the action could only be instituted by the paying bank the argument in support was that; as it were under **Foley V. Hill**[19] the contract of Banker and customer constituted a contract of debtor and creditor, thus money paid to the credit of the customer account became, accordingly the bank's money. How then could a customer, who had no title to the money in question bring an action based on it having been paid out under a mistake of fact?. This reasoning was challenged in two cases and notwithstanding this doctrine in **Foley V. Hill** the customer has a right to bring an action for the recovery of funds paid out by the bank under a mistake of fact.

In **AGIP (Africa) Ltd. V. Jackson**[20] the plaintiff sought to recover in an action in restitution large amounts of money fraudulently transferred by its chief accountant to the credit of accounts maintained by the defendant using **EFT** transactions **Millet J** at first instance, rejected the plaintiffs common law action for money had and received against the

---

[18] C.REED consumer Electronic Banking (1994) 11 JIBL 451, 462

[20] (1990) Ch 265, affd (1991) ch 54

defendants who had received the misappropriated funds into their banks accounts; he went further to say that ..... By honoring the customer's order in favor of a 3rd party and debiting his account, the bank acts as the principal in repaying part of the debt to its customers and as agent of the customer in paying his money to the third party" he went further to state that "the position was not altered by the fact that in the instant case the paying bank had paid the money in reliance on a fraudulent instruction and hence without a genuine mandate. If the bank paid out **Agips** money, **agip** itself must be entitled to pursue such remedies as there may be for its recovery.

The second case is **Lipkin Gorman vs Kapnale Ltd**[21] where a partner in a firm of solicitors used money he had obtained through a fraudulent transaction to gamble at the defendants club. The defendant lost over half of the US Dollars 323,222.14 at the club. Reversing the decision of the court of appeal. House of Lords held that the solicitors firm was entitled to recover from the defendant the net amount lost by the partner. **Lord Goff of Chiveley** said at 573.

"Before he drew upon the solicitors client account at the bank, there was of course no question of the solicitors having any legal property in any cash lying at the bank. The relationship of the bank with the solicitors was essentially that of the debtor and creditor and since the client account was at all material times in credit, the bank was a debtor and solicitors creditor."

3.1.4 COUNTERMAND AND COMPLETION/TIME OF PAYMENT

Looking at the relationship between countermand and payment completion, it is very clear that at whatever point of the payment process, or payment instruction becomes irrevocable, it cannot be later than the point of legal completion of payment. In theory, the two points may meet but in practice they may well not do so.[22]

The analysis of the legal relationships of the parties to money transfers does not furnish a decisive answer to the question of when the order is executed. An attractive argument is that the order is performed when payment is complete, in the sense that there

---

[21] (1996) 2 A. C 548
[22] Ibid No. 16

is no longer room for a countermand. Unfortunately, this answer leads to circularity, as, on the same basis, payment is complete and a countermand precluded when the order is expected upon the receipt of the funds by the payee or his agent, the recipient bank. First and foremost, it is essential to have regard to the nature of the money transfer operation involved. In some cases the master agreement between the banks and the customers determines the time at which an instruction to transfer becomes irrevocable. Secondly, the time of payment may depend on the number of parties involved in the transaction and on the role assumed by each one of them. At one end of the scale there is the in-house transfer, in which the payee and payer maintain their accounts with the same branch of a given bank.

An answer to the problem of countermand and completion of payment is influenced by the practical situation in which they arise. This is so because the position of the recipient bank varies from transaction to transaction as to when an EFT transfer is executed. In some cases where the transferring bank wishes to stop payment or reverse a credit entry, the payee is likely to maintain the payment has been completed before the attempt to countermand is made. All in all, in every case coming up for decision there are, basically, six points of time at which payment may be regarded as executed.[23] The first is the time at which the payer's instruction is transmitted by the transferring bank. The second is the time at which the instruction reaches the recipient bank. The third is the time at which the recipient bank sets in motion the internal machinery for crediting the payee's account. The fourth is the time at which the payee's account is credited with the amount involved. The fifth is the time at which the payee is notified of the receipt of the funds. The sixth is the time at which the payee agrees to receive the amount involved, either expressly or by implication.

Attempts to countermand money transfers, or to question their execution, arise in different circumstances. The earliest decision in point is **REKSTIN V SEVERO SIBISKO GOSUDARSTUENNOE AKCIONERNO OBSCHESTVO KOM SEVERPUTJ.**[24] Where a

[23] BAKER, law of EFTs Pg. 29 – 21 – 29 – 27 who suggest similar points of time
[24] (1933) I KB 47

customer instructed his bank to transfer the balance standing to his credit to an account maintained with the same bank by another customer. After the bank had effected the transfer by making the required ledger entries but before notification was given to the payee, a judgment creditor served a garnishee order nisi attaching the transferors balance. It was held that, at the time the order nisi was served, the amount transferred was still accruing to the transferors as there was no evidence to establish their assent to the transfer. The bank could not be held to have authority to hold the amount as debt accrued to him. This decision is held in modern times to lack strength because most banks today are given authority for the crediting of the payee's account by implication.

The importance of determining the moment at which payment is accrued to the payee is demonstrated by the leading English decision in point **Momm v. Barclays Bank International Ltd**[25] The defendant bank received instruction from one of its customers, the herstatt bank of Frankfurt, to credit the account of the plaintiff, another customer of the same bank, with an amount of $120,00. Although the herstatt account did not have an adequate credit balance, the manager decided to credit the plantiffs account. Later in the day herstatt suspended payment. On the next day the defendant bank reversed the credit entry which had appeared in the plaintiffs account. The plantiff was never notified but discovered the facts through a perusal of the defendants bank's books. He brought an action for a declaration that his account had been wrongfully debited on 27th June. Giving judgment for the plaintiff **Kevv J** treated the credit entry in the plaintiffs account with the defendant bank as a final settlement, or payment although there was no proof that the plaintiff had authorized the defendant bank to receive payment. His lordship emphasized that the payment would be final only if it stood undisturbed at the end of the 'value date' which is the date on which funds are to be made available to the payee.[26]

These two cases show that a transfer is complete when the funds are made available to the recipient bank and accepted by it unilaterally on the payee's behalf. This view derives support in the case of **LIBYAN ARAB FOREIGN BANK vs**

---

[25] [1977] QB 790

[26] cf libyan arab foreign bank vs. bankers trust co (1988)1 Llyods Rep. 259,273 – 4 where Straugton J inclined to the view that payment our in-house transfer was complete when the bank set the transferring into motion. The observation though was obiter

MANUFACTURERS HANUVER TRUST CO.[27] In respect of a money transfer effected between accounts maintained by two separate branches of the same bank. His lordship, **Hirst J** concluded that the transfer was complete when the transferring bank branch debited the recipient branch's account with itself and latter branch effected a matching bonafide credit entry in the payee's account. This means that the transfer was complete and irreversible when funds were made available to the payee.

In case of an inter-bank transfer, where funds are transferred between accounts held at different banks, payment between the payer and payee is complete when the receiving bank receives payment instructions from the paying Bank and decides to make an unconditional credit to the payee's account in the equivalent amount, assuming that the receiving bank has the payee's actual or ostensible authority to accept the transfer on his behalf.[28] It does not matter that the receiving bank has yet to credit the payee's account or notify him of the transfer.

In **Mardorfpeach & Co Ltd V Attica sea Carriers Corpn of Liberia, the laconia**[29] where owners of the ship rejected late payment of hire. Charterers argued that their breach had been waived through acceptance of late tender by the owners' agent i.e. the bank. The House of Lords reversing the court of appeal rejected the contention and decided in favor of the owners. Their lordships held that the bank only had limited authority to waive the owners' rights to withdraw the vessel. Although the bank had begun to process the payment order, it was held to be purely provisional and reversible.

3.1.5 CONFIDENTIALITY AND DATA PROTECTION

The use of computer technology by banks and other **EFT** system providers facilitates the collection, storage and dissemination of customers' information. However as this duty arises only when the relationship of a banker and customer is established, it would not extend to information acquired by an **EFT** system provider, although these bodies may

---

[27] 1 Llyod's Rep. 608, 631 - 2
[28] a/s awilco of oslo vs. fulvi spadi navigazione of calgari the ctrikoma (1981) 1 WLR 314
[29] (1977)AC 850

acquire the information in circumstances which gives rise to an equitable duty of confidence.[30]

Under the common law, the bank owes its customer a contractual duty of confidentiality. The information which the bank is bound to treat as confidential, is not restricted to facts that it has learnt from the state of the customers account. The duty encompasses information obtained from other sources than the customer's actual account. The occasion upon which the information is obtained, should be out of banking relations of the bank and its customer.[31]

Although common law is well developed and that Kenyan courts will still have to apply it before a more definite law on confidentiality is established, privacy and confidentiality are still a great concern to the whole world. How banks collect, use, control, correct or abuse that information is becoming a critical issue with consumers.

In the US the Federal Trade Commission (FTC) has surfed the websites of 100 (hundred) banks to search for privacy and confidentiality principles and determine how those banks purport to handle the information they gather about consumers. Initial reports suggest that FTC is dissatisfied with what it has seen.

There is no central source of privacy protection in Kenya. The constitution does not create a substantive right of privacy. There is a need for a Data protection Act in Kenya which will regularize confidentiality in **EFT** transactions as it would regulate the use the computerized data by both banks and other institutions involved in **EFT** process.

CONCLUSION

As the new technologies develop into new ways of making payment, one concern naturally arises. Will this technology protect individual rights while providing the sound money needed for the economic health of communities? The answer is simple – it depends on how the new technology is used. There is nothing inherent in the technology

[30] A. G. vs. Guardian newspapers (N0.2) (1990) A. C. 109
[31](1924) 1 KB 461,48 TOURNIER CASE

that makes it less protective of privacy and individual rights. In fact, advancements such as PGP (pretty good privacy) make individual privacy even more secure.

As developments in electronic money gather pace, protection of individual rights must be kept in focus. Because the record of most governments so far in these early stages of electronic banking has been seen by many to be confrontational and not protective of individual rights, it is likely that the preservation of these rights is one reason that private currencies are likely to emerge on the Internet and to eventually play an important role in global commerce.

Clearly, the field is wide open for any entrepreneurs who want to create a private currency. The technology now exists so that anyone with a few hundred thousand dollars (may be less) can set up a working and robust digital currency system. Slowly, but surely, private currencies will begin to emerge.

Competition between currencies whether government or private is beneficial to everyone in the digital economy. The currencies of substance that maintain value over time and are implemented under a trustworthy and secure computer and communications system will be the ones that will circulate and be accepted globally.

CHAPTER 4

REGULATION OF EFT'S IN OTHER COUNTRIES: A COMPARATIVE STUDY

4.0 THE EUROPEAN COMMUNITY (E.C)

Member states in the E.C planned to move to a single internal market by 1992. They achieved this by means of a 1987 Act[1], which was ratified by member states and their respective parliaments.

"Unifying this market (of 392 million people) presupposes that member states will agree on the abolition of barriers of all kinds, harmonization of rules, approximation of legislation and tax structures strengthening of monetary co-operation and the necessary franking measures to encourage European firms to work together".[2] In pursuit of this aim Electronic Banking was one of the main areas that technical difficulties, and barriers, had to be done away with. The E.C had a three tier co-ordinated approach to the problem. The first an overall policy paper[3]whose general thrust was interoperability of EFT transactions as a whole to ensure systems in one member state are compatible with systems in other member states. More specifically the paper sought for standardization of agreed procedures for hybrid inter-accessible networks, standards. There was a need for E.C to develop a system of EFTS capable of competing with the U.S.A. and Japan in the same field.

The second was through a Recommendation[4] that appropriate measures be taken that issues of payment devices and system providers draw up full and fair terms of contract, in writing, governing the use of Electronic Fund Transfer systems. The terms of contracts should include the security system, written records of the transaction; provisions that in a dispute transaction, the burden of proof should be on the bank or financial institutions, provisions limiting the liability of the customer unless he has acted in extreme negligence; among others, however there is no provision for any dispute resolution mechanisms.

---

[1] Single European Act of 1987
[2] "Completing the internal market", The Europeans Commision's 1985 white paper
[3] "Europe could pay on Ace: The new payment cards", presented to the E C in 1987

Thirdly in 1987, a code of conduct was issued[5] this effectively gave a statement of principles covering relations between banks, traders and service establishments and consumers. It required all contracts to be in writing and stipulated that transparency in charging arrangements and irrevocability of payments. The code also provides that banks at all times should comply with the Data protection Act 1984 when obtaining and processing customer's information.

4.1 U.S.A.

Banks in the U.S.A. were until recently prohibited from having full- service offices in more than one state, but are still restricted in their geographical scope within U.S.A. But there are nationwide-shared EFT networks that have so far been the main area of application of U.S. law[6]

Explicitly a piece of consumer protection legislation[7] this Act effectively covers EFT transactions. Among other things it requires banks to disclose terms and conditions of any EFT transactions when the customer first contracts for it, and to give him at least 21 days notice of contract variation; stipulates written documentation for each transfers, sets out procedures for error resolution; and in the case of unauthorized transfers, places the burden of proof on the bank, and limits the customers liability, in any event.

The Act is translated into practical working rules for the bank by means of federal Reserve Boards, Regulations[8] which are amended from time to time. The "Fed" has the task of administering the Act overall, apparently they are first involved in consumer protection and in the resolution of customers' disputes with their banks.[9] congress chose to enact this legislation at time when EFT transactions and their problems became widespread, with the twin aims of boosting consumer confidence and of encouraging banks to improve security to their systems. Doubts have indeed been voiced in other jurisdictions about the wisdom of applying inflexible statute law to the context of such rapidly changing technology. These doubts are however discounted by both authorities and operators in the

---

[4] Ec recommendation of 17th November 1988 concerning payment system
[5] European code of conduct on Electronic payment of 1987
[6] USA's Electronic funds Transfers Act of 1978
[7] Ibid. preamble
[8] Regulation E.

U.S.A. They argue that flexibility is preserved by the device of regulation E which has already been amended extensively. U.S.A. banks themselves pressed for EFT legislation from the start believing that their systems could be more acceptable to customers if they were assured protection of the law. At all events the Act has served as a model for EFT rules of one kind or another in different jurisdictions.

The USA has got other statutes that deal with EFTs in their provisions. The uniform commercial code[10] is one such legislation. It deals with the rights and obligations of banks between themselves on EFT transfers. The rights and obligations which are contractual, can be varied by contracts of the affected parties, arise from acceptance by a bank of a payment order issued to the bank. Until that acceptance occurs the issue of a payment orders does not create rights and obligations.

The risk of loss from unauthorized payment is to be allocated in accordance with a security procedure agreed in advance by a customer and the bank provided that it is a commercially reasonable security procedure. There are also sections dealing with liability for improper execution or failure to execute and with special procedures to reduce the risk faced by collecting banks using the local systems. Other acts in the USA deal with various EFT problems including the delay imposed by many banks in making proceeds available[11]the USA has the most modern and expeditious law covering EFT transaction in the world today.

4.2 AUSTRALIA

Recent developments in Australia have a certain pioneering flavor. The Australians have been the pioneers of a code of good practice of EFT. Its scope though is narrower than the U.S.A. EFT legislation. The code of good practice[12]covers issues and use of EFT transactions i.e. funds transfers made through electronic channels. On the whole, the code is similar to the US act[13]for which the Australians seem to have poached ideas. These ideals include consumer protection measures.

---

[9] Ibid
[10] Article 4A
[11] Expedited funds Availability Act of 1987
[12] Issued in 1986
[13] Supra

However the code does not place a burden of proof in case of disputed transactions on either party. but associated reports of officials makes clear that a responsibility exists to resolve disputes on the basis of established facts not on inferences. The Australians have set a limit on customer liability in cases of disputed EFT transactions.

The code of good practice seems to have come about partly because of the active role played by the Australian consumer bodies in the banking field and because the government saw it proper to balance market imperfections during a period of deregulation. The government merely plays a monitoring role[14]

This light touch in Australia has worked in their context with all major institutions complying with the code and it has led to a marked improvement in terms and conditions of their customer contracts, as well as a reduction in customer complaints. New developments centered on customer information on the code and implementation of new security measures were to be incorporated in the Amended and reviewed code of conduct in 1999

4.3 UNICITRAL

The United Nations commission on international trade Law based in Vienna completed a study in 1992 known as UNCITRAL model law on International credit transfers[15] which was "prepared to aid legislators and lawyers considering the rules of particular networks..... to find out the common elements in the law and the banking practice of funds transfer"[16] among member countries.

The approach followed by the legal guide was to first identify 41 legal issues arising out of EFT systems on a very broad definition of EFTs[17] a funds transfer in which one or more techniques are now done by electronic techniques. Examples were whether changes in the law are required through development of EFTs, whether there should be a legal

---

[14] Through the state consumer affairs minister

[15] On 25th November 1992, by resolution 47/34 the United Nations General Assembly approved the report on UNICITRAL and the model law on international Credit Transfers finalized at UNICTRALS 25th session of 4 – 22 May 1992.

[16] Ibid

[17] Supra

requirement us to the form of authentication necessary in the system and whether the bank or customer should carry the burden of proof in the case of a disputed transaction.

The legal guide is a valuable work of reference, offering a wider perspective to any would be national regulator in the EFT field. The model rules are mainly concerned with EFT transfers but the main forms of interest appears to be on completion of payment by posing the questions whether there should be a single point of time when a funds transfer instructions should be considered to be complete for all legal purposes and whether there are several transactions in a funds transfer or there should be a separate completion rules for each transaction.

CHAPTER 5

RECOMMENDATIONS

"There is an urgent need to develop banks which can act as competent and reliable agents of development. There is also in existence a need to have a banking system that has integrity beyond any doubt so as to command the full trust and confidence of the customers"[1]

These words by the presidential commission inquiring into the banking system in Tanzania to capture the true picture of the objective of any reforms that need to be undertaken on the banking system in any country, Kenya included. The aim of such reforms should be to safeguard the greatest asset that monetary institutions can ever possess i.e. the full trust and confidence of the customers.

This paper has sought to highlight some of the issues arising in the banking industry today, and how the law can be used to provide solutions. The function of law in banking is to provide a legal framework for the provision of banking services on fair and efficient terms. At present, this is done under the common law frame work, but the nature of banking has changed almost beyond recognition over the years since the common law principles were established and there is need for a new law which takes into account technological and other developments. Looking at the laws in other countries, which have undergone similar revolutions in banking, provides at least a starting point for a new legal regime in Kenya.

In general legal intervention in Kenya tends to be a reaction to specific social problems which periodically arise, rather than a programmed pattern of response to institutional questions[2]. Reform of banking law usually favors some sort of crisis, such as collapse of banks. However the need for an inquiry into banking services, law and practice does not have to stem from deep public disquiet, and reform need not always come in the wake of some dramatic event. For instance, reform of banking law in the UK has been

---

[1] Report and recommendation of the presidential commission of inquiry into the monetary and Banking system in Tanzania submitted to President A. H. Mwinyi on July 11th 1990

[2] Okech - Owiti: Regulating Technology : The case of computers in Kenya in innovation and sovereignty. The patent debate in African Development at Pg. 193 to 195

prompted by a generalized concern about developments on the banking scene and growing doubt as to whether the traditional framework was wholly adequate to meet the problems posed by those developments.

The law must strike a balance between the reasonable requirements of any bank for freedom to operate commercially and the no less reasonable requirement of its customers, perhaps with weaker bargaining power for the basic protections the law should give them In the ordering of their private financial affairs. It should be pointed out that the need for reform does not mean that a fresh start and an entirely new legal framework is called for. Substantial parts of the common law tradition have stood the test of time. With the future pattern of banking services still uncertain there is a danger that a wholesale new law would get some things wrong. A balance must be struck between the need, on the one hand, to repair shortcomings in the existing law and to bring standards of banking practice up to date, and on the other, to preserve continuity and maintain some consistency within the law.

5.1 PROPOSED FRAMEWORK FOR A NEW LAW

New solutions to problems of law and practice in the electronic banking services field should give priority to the following objectives:.

CONSUMER PROTECTION AND FAIRNESS OF CONTRACTUAL TERMS

Development of the economy requires that innovations be introduced, but the rights of the consumer should remain paramount. After all development is not just about greater efficiency and productivity. It is also about enhancing fairness and protecting weaker parties'.[3]

Parliament should therefore enact a statute that will regulate the use of standard contract terms, taking care to reconcile the need for speed, certainty and predictability in

---

[3] NDERITU, E. M in Consumer protection in Kenya: Theory and Practice Okech - Owiti , Ed. Unpublished manuscript (1996)

contracting and the requirement for fairness to the consumer.[4] This legislation should be expressly for purposes of consumer protection so as to replace the money lenders Act, with provisions designed to protect the borrower or user of **EFT** services especially in view of the importance of EFTs and the fact that the borrower rarely has any say with regard to the terms of the agreement.

Such legislation is vital because at present there is no law regulating the fairness or otherwise of the terms of the EFT contract or negotiations leading up to the contract. Courts have so far not been able to formulate rules, which can effectively be used in policing unfair terms in standard form contracts.

To ensure that any new legislation does not hamper growth, it has been suggested that it should draw a distinction between regulations protecting the general public and those applicable to the professional and financially sophisticated community. This would be an appropriate compromise between the needs of consumer protection and financiers who feel that the state should not be too paternalistic.

5.2 BANKING SERVICES ACT

The banking services Act should seek to create certainty in areas of law which are not yet settled. For instance, there should be a consistent legal rule to determine the point at which payment in an EFT is complete, and this rule should apply in all cases where the contract itself does not make explicit provision on the matter.

The Act should confer on customers a right of access to computer records about themselves held by banks, and require banks to inform the customer, by means of leaflets or other suitable means, of this right. Banks should have a statutory duty to seek the customer's consent before divulging information about him in cases where his interests will be prejudiced by this divulgence, if the case does not fall within the exceptions laid down in

[4] The middle Africa Group Vol. No. 4 April 1995

TOURNIER'S CASE.[5]

In cases arising from unauthorized operations on the account, the legislators should borrow a leaf from overseas precedent[6] whose provisions limit the customers' liability for loss arising through unauthorized transactions or systems malfunctions. Also the act should provide for the equitable allocation of loss where a question arises on who activated the EFT transaction.

5.3 THE CENTRAL BANK OF KENYA ACT

This statute was enacted to establish the CBK, to provide for the operation thereof and related matters. S.4A (d) empowers the Bank to "promote the smooth operation of payments clearing and settlement systems". This provision is drawn in general terms and is proposed that the Act be amended to specifically empower the bank to perform such functions, implement such rules and procedures necessary to establish, conduct, monitor regulate and supervise payments, clearing and settlement systems.

An important component of the central bank's leading role is to create an organizational structure to coalesce domestic and external actors, functions and interests. The CBK must take the initiative and set up a **National Payments Council.** (NPC) to lead payment Systems reform. The NPC must be à forum (talking shop) for the central and commercial bank's to discuss and agree on how to establish and oversee the functioning of the National Payment System (NPS) and how to coordinate central and commercial banks' policies in the payment system.

5.4 THE EVIDENCE ACT

This act declares the law of evidence applicable to all judicial proceedings in Kenya. The purpose of **Chapter Vii** of the act is to ease the process of producing banker's books as evidence in court. **S. 176** allows banks to produce copies of their books as prima facie evidence of entries made in them. Although the use of electronic media in the process of banks and the electronic preservation of records is currently in practice in the banking

---

[5] (1924) IKB 461

industry particularly, the act does not provide for the electronically generated and stored material. Thus the Act should provide for that.

5.5 A CODE OF CONDUCT

Historically, the development of standards of best banking practice has been the sole prerogative of banks. But competition while increasing with closure of many banks and bank branches cannot be relied upon entirely as appropriate to come up with such a code. The legitimate public interest in those standards alone requires some objective assessment of their adequacy.

The Kenya Bankers Association should, with the help of consumer groups come up with code of conduct. Though such a code need not be promulgated in one document at first, it will subsequently be one document covering all areas of Banking Services. This code should give priority to the noble EFT area. A standard should be set for authentication of customer's instructions so as to meet a certain minimum standard of security.

This code will supplement the Banking Act. Despite the code not having the force of law, it will enable the industry to be more self-regulatory. All members would have an interest in adhering to the rules, which they have devised. This code will provide the basic framework of conduct, which will ensure that the banking regulations on EFT are followed.

---

[6] The UK's Consumer Credit Act of 1974.