"THE LEGAL AND REGULATORY FRAMEWORK IN KENYA IS INADEQUATE TO ADDRESS THE LEGAL ISSUES ASSOCIATED WITH INTERNET BANKING: THE CASE FOR REFORMS BASED ON THE BEST PRACTICES IN OTHER JURISDICTIONS."

BY NDIRANGU FRANCIS KIAGO.

G62/76638/2009.

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF LAWS (L.L.M) OF THE UNIVERSITY OF NAIROBI.

NAIROBI SEPTEMBER, 2012

DECLARATION

I, **NDIRANGU FRANCIS KIAGO**, do hereby declare that this is my original work and has not been submitted and is not currently being submitted for a degree in any other University.

SIGNED..... **Date** 5/12/2012

NDIRANGU FRANCIS KIAGO.

This thesis has been submitted with my approval as the Supervisor.

SIGNED..... **Date** 5/12/2012

MRS PAMELA AGER

LECTURER, SCHOOL OF LAW

UNIVERSITY OF NAIROBI.

ACKNOWLEDGMENT

I would like to express my profound gratitude to my Supervisor, Mrs. Pamela Ager who gave me invaluable assistance, guidance and insightful comments in writing this thesis. Your critical thoughts and support went a long way.

I would also like to thank the University of Nairobi for giving me such a timely opportunity to undertake my Masters course. Special thanks to the Parklands Law School community, class of 2009/ 2010 and the Board of Postgraduate Studies.

Finally, I would like to thank the greater Ndirangu family, Mr. John Ndirangu, Mrs. Nelius Nyakieni Ndirangu, Anne Njambi, Carolyne Wangeci and Natasha Wambui, for their undying love, support and encouragement.

DEDICATION

This project is dedicated to my entire family, especially my parents, who encouraged and urged me on in more ways than I could ever imagine, during the course of my postgraduate studies.

ABSTRACT

Since the late 1990's the internet and other technological advances in telecommunications, information technology and computer software and hardware have transformed the provision of financial services and the structure of financial markets.

Internet is increasingly used by banks as a channel for receiving instructions and delivering their products and services to their customers. The range of products and services offered by different banks vary widely both in their content and sophistication

From the perspective of banking products and services being offered through internet, internet banking is nothing more than traditional banking services delivered through an electronic communication backbone, through the internet. But in the process it has thrown open issues which have ramifications beyond what a new delivery channel would normally envisage and hence has compelled regulators world over to take note of this emerging channel.

Some of the distinctive features of internet banking are:

1. It removes the traditional geographical barriers as it could reach out to customers of different countries. This has raised the question of jurisdiction of law / supervisory system, to which such transactions should be subjected.
2. It has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges.
3. Security of banking transactions, validity of electronic contract and customers' privacy have assumed different dimensions given that internet is a public domain, not subject to control by any single authority or group of users and

4. It poses a strategic risk of loss of business to those banks who do not respond in time to this new technology, being the efficient and cost effective delivery mechanism of banking services.

The world over, central bankers and regulators have been addressing themselves to meet the new challenges thrown open by this form of banking. The thrust of regulatory thinking has been to ensure that while the banks remain efficient and cost effective, they must be aware of the risks involved and have proper built-in safeguards, machinery and systems to manage the emerging risks. This can only be done guided by an appropriate legal and regulatory framework to address the above legal and regulatory issues associated with internet banking. The central question for legal practitioners and lawmakers revolves around how to accommodate the use of new technology in banking and financial services in the already existing law and how to regulate it from a concrete and clear legal perspective.

There is no specific law that deals with internet banking in Kenya. The Constitution and various Acts of Parliament capture different aspects of the law. The law applies generally without specific reference to electronic banking or internet banking. Accordingly, any legal and regulatory framework to govern internet banking should at the minimum revolve around the setting, enactment and enforcement of a set of laws comprising:

a) Law on Electronic and Digital Signature
b) Law or Regulation on third-party Certification Authorities
c) Laws or Regulations on e-Banking per se
d) Law on Data Privacy
e) Laws on Anti-Money Laundering.

The above set of laws will act as a benchmark when examining the current legal and regulatory framework governing internet banking in Kenya with a view of identifying the gaps and the legislative and regulatory reforms that are necessary to bring it at par with international best practices in other jurisdictions.

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
ATM	Automated Teller Machines
ARPANet	Advanced Research Project Administration Network
ARCC	African Regional Centre for Computing
CBK	Central Bank of Kenya
CCK	Communications Commission of Kenya
EAC	East African Community
E- BANKING	Electronic Banking
E- BANK	Electronic Bank
E BRANCHES	Electronic Branches
E- COMMERCE	Electronic Commerce
EDI	Electronic Data Interchange
E- FINANCE	Electronic Finance
EFT	Electronic Funds Transfer
EFTPOS	Electronic Funds Transfer at Point Of Sale
E PAYMENTS	Electronic Payments
E- TRANSACTION	Electronic Transaction
EU	European Union
E SIGN	Electronic Signature in Global and National Commerce Act
FATF	Financial Action Task Force
FSA	Financial Services Authority

FSMA 2000	Financial Services Markets Act
I-BANKING	Internet Banking
I-O-B	Internet Only Bank
ICT	Information Communication Technology
IT	Information Technology
ISP	Internet Service Provider
IP	Internet Protocol
ITU	International Telecommunications Union
KES	Kenya Shillings
MAS	Monetary Authority of Singapore
NSF	National Science Foundation
OECD	The Organisation for Economic Co-operation and Development
PC	Personal Computer
TCP	Transmission Control Protocol
TTP	Trusted Third Party
UETA	Uniform Electronic Transaction Act
USA	United States of America
UNICITRAL	United Nations Commission on International Trade Law

TABLE OF STATUTES

Kenya

The Banking Act, Chapter 488 Laws of Kenya.

The Constitution of Kenya 2010.

The Central Bank of Kenya Act, Chapter 491 Laws of Kenya.

The Kenya Information and Communications Act, Chapter 411A Laws of Kenya.

The National Payment Systems Act, No 39 of 2011 Laws of Kenya.

The Proceeds of Crime and Anti-Money Laundering Act, No 9 of 2009 Laws of Kenya.

The Consumer Protection Bill 2011

United Kingdom (U.K)

The Financial Services and Markets Act 2000.

The Electronic Communications Act 2000.

The Data Protection Act 1998.

United States of America (U.S.A)

The Federal Reserve Act.

The Uniform Commercial Code (UCC).

The Uniform Electronic Transaction Act (UETA).

The E-sign Act.

The Right to Financial Privacy Act 2009.

The Bank Secrecy Act (BSA).

The USA Patriot Act.

Singapore

The Monetary Authority of Singapore Act.

The Banking Act.

The Financial Advisers Act.

India

The Reserve Bank of India Act 1934.

The Banking Regulation Act 1949.

The Information Technology Act 2000.

Payment Settlement Systems Act 2007.

TABLE OF CASES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.0 Background

There are not many inventions that have changed the business of banking as quickly as the e-banking revolution. E-banking has enabled banks to scale borders, change strategic behaviour and thus bring about new possibilities. This path has been forged partially due to the growing acceptance of Internet banking .[1]

Since the late 1990's the internet and other technological advances in telecommunications, information technology and computer software and hardware have transformed the provision of financial services and the structure of financial markets. By the end of the 1990's, electronic finance applications had influenced most aspects of the business of banking. Although the advent of electronic finance has rightly been associates with the most recent applications of advanced technologies in the financial services industry, in strictly technical terms e-finance predates the era of the internet by several decades: the first era of electronic banking in the form of telegraphic fund transfers in the late 19th century gave rise to legal problems that would appear familiar to electronic banking lawyers today. [2]

Internet has evolved to its present state out of a US Department of Defence project ARPANet (Advanced Research Project Administration Network), developed in the late 1960s and early 1970s as an experiment in wide area networking. A major perceived advantage of ARPANet was that the network would continue to operate even if a segment

---

[1] Rupa Rege Nitsure, "E- banking: Challenges and opportunities," Economic and Political Weekly 38 No 51/52(Dec. 27, 2003 - Jan. 2, 2004): p5377. <http://www.jstor.org/stable/4414436> Accessed: 02/07/2010.

[2] Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Integration and Electronic Commerce*' (Cambridge University Press, 2006), p7: See *Bank of British North America v. Cooper,* 137 US 473(1890) (liability for negligent performance of a transatlantic wire funds transfer).

advantage of ARPANet was that the network would continue to operate even if a segment of it is lost or destroyed since its operation did not depend on operation of any single computer. Though originally designed as a defence network, over the years it was used predominantly in areas of scientific research and communication. By the 1980s, it moved out of Pentagon's control and more independent networks from US and outside got connected to it. In 1986, the US National Science Foundation (NSF) established a national network based on ARPA protocol using commercial telephone lines for connectivity. The NSFNet was accessible by a much larger scientific community, commercial networks and general users and the number of host computers grew rapidly. Eventually, NSFNet became the framework of today's Internet. ARPANet was officially decommissioned in 1990.[3]

Internet is increasingly used by banks as a channel for receiving instructions and delivering their products and services to their customers. The range of products and services offered by different banks vary widely both in their content and sophistication.

Electronic banking can be defined as the provision of banking services and the initiation and performance of payments through the banking systems by electronic means and other advanced technologies. Electronic banking is a conceptually generic term, which denotes banking services provided through a variety of access devices and links of communication.[4] (See figure 1.1)

Internet banking refers to the provision of electronic banking services via the internet, commonly through a personal computer (PC) or other access device with Internet

---

[3] Shri S. R Mittal& others, "Report on Internet Banking", Working Group set up by Reserve Bank of India, June 2001:p8<http://www.rbi.org.in/scripts/PublicationsReportDetails.aspx.> Accessed 5/09/2012

[4] Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Integration and Electronic Commerce*', p7.

capabilities.[5] Online banking and Internet banking are often used interchangeably. Internet banking gives the customers the ability to access virtually any type of banking services (except cash) in any place and at any time.

From an economic perspective, information technology and computer networks have enhanced the automation, speed and standardization in communications and internal administration, increasing customer convenience and functionality and reducing costs of back-office and front-desk banking functions.[6]

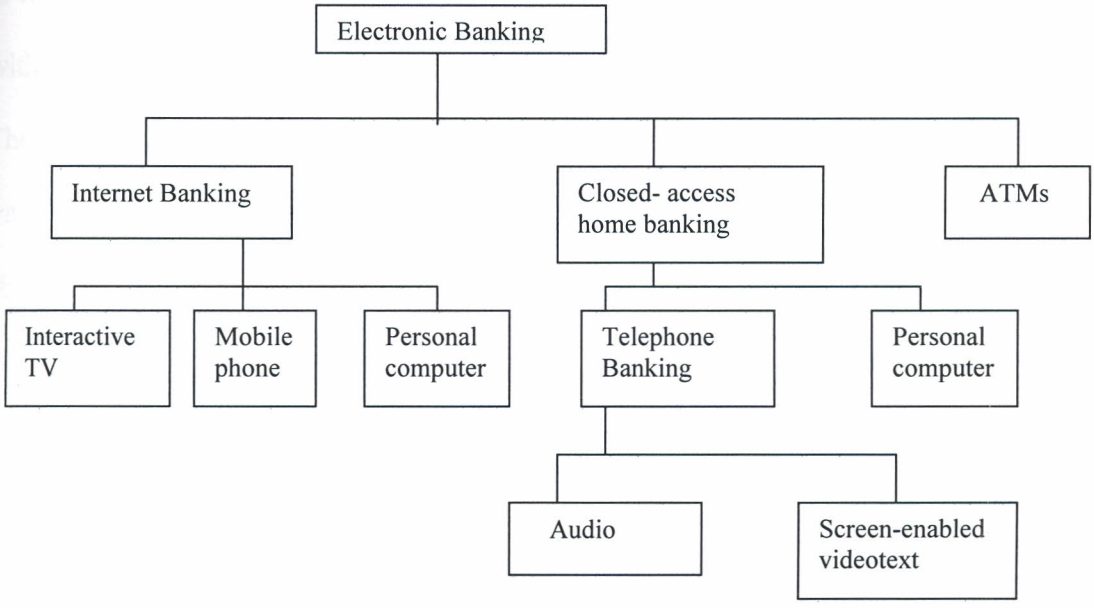

Figure 1.1. Communication methods and access devices in electronic banking.

The two prevalent internet models in the banking industry are e-banks and e-branches.[7] An e-bank is a banking institution that exists only on the internet, with no bricks-and mortar branch access. E- bank can also be referred to as "Internet-only" bank or virtual

[5] Ibid,p8

[6] Allen Berger, 'The Economic Effects of Technological Progress: Evidence from the Banking Industry'(2003) 35 *Journal of Money, Credit and Banking*:p141 <http:// www.federalreserve. gov /pubs /feds/2002/200250/200250pap.pdf> Accessed: 8/09/2011.

[7] Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Integration and Electronic Commerce*', p23.

bank. This framework gives a bank the opportunity to exist without paper, without geographical limitations, and without ever closing the doors to customers. The computer server that lies at the heart of a virtual bank may be housed in an office that serves as the legal address of such a bank, or at some other location. These banks may offer their customers the ability to make deposits and withdraw funds via ATMs or other remote delivery channels owned by other institutions.[8]

The e-branch model is where a traditional bricks-and-mortar bank offers Internet banking to its customers. The bank will construct a web site and offer Internet banking, together with traditional banking.[9]

The internet banking web sites can either be informational, communicational, or transactional.[10] Informational web sites are intended to disseminate general information about the banking institution and to advertise its products and services. This websites offer basic level service and it may receive and reply to customers queries through e-mail. Regulation of these types of web sites is less as the risk of privacy and security breaches are minimal.[11]

Communicational web sites allow interaction between a bank and its customers to a certain extent. They allow customers to submit their instructions, applications for different services, queries on their account balances, etc, but do not permit any fund-based transactions on their accounts. The communicational web site has some risk attached to it as the transmission of computer messages may be infected by viruses.

---

[8] Ibid.
[9] Ibid.
[10] Sarabdeen Jawahitha, Noor Raihan Ab Hamid and Mohamed Mazahir Mohamed Ishak, " Internet Banking: A Comparative Analysis of Legal and Regulatory Framework in Malaysia," Arab Law Quarterly, 18, (No. ¾) (2003): p293. Published by: BRILL <http://www.jstor.org/stable/3382038>.Accessed: 08/09/2011.
[11] Ibid

These viruses may affect the internal network or they can transmit confidential information from the bank's server to the sender of the virus.[12]

Transactional web sites allow customers to perform most of the transactions that they can perform in a brick-and-mortar bank. They allow the customers to operate on their accounts for transfer of funds, payment of different bills, subscribing to other products of the bank and to transact purchase and sale of securities. The transactional web site, unlike the other web sites, invites more of a threat as it provides links to internal networks and computer systems.[13]

Internet banking have achieved significant market penetration in most developed countries and key emerging markets and demonstrate potential for further growth (see table 1.2). It appears that higher income and higher market acceptance of electronic finance are strongly correlated. This probably reflects the link between high income and good IT resources and skills. According to the directly of European banks maintained by Qualisteam,[14]over nine hundred depository institutions across Europe perform services over the internet. Customer acceptance of the business model is also high and rising. In Europe one in five customers performs transaction over the internet and figure rises to one in four among internet users.[15] The service is particularly popular in the Scandinavian and Nordic countries. It appears that education, age and profession are the most influential demographic variables, alongside income, of customer acceptance. The typical

---

[12] Ibid

[13] Ibid

[14] See http://www.qualisteam.com/Banks/Europe/index.html. Quoted in Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Intergration and Electronic Commerce*':p20

[15] See Centre for the Study of Financial Innovation (CSFI) (ed.), *The New World of Europe E- Finance* (London, 2002) , p 47. Quoted in Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Intergration and Electronic Commerce*':p20

user is profiled as a degree holder, aged between twenty-three and forty-six, urban, professional and with a relatively high income.[16]

Table 1.2 *Penetration of Internet banking (end of 2000)*

Income group/economy	Internet banking (% of total bank customers)
Industrial country average	**8**
Australia	4
Belgium	4
Denmark	6
Finland	20
France	2
Germany	12
Netherlands	15
Norway	8
Portugal	2
Singapore	5
Sweden	31
United Kingdom	6
United states	6
Emerging markets average	**5**
Brazil	5
India	11
S. Korea	13

Source: S Claessens et al., Electronic Finance: A new Approach to Development (Washington, DC: World Bank, 2002)

[16] See Hans Christiansen, Electronic Finance: Economic and institutional Factors(Paris: OECDFinancial Affairs Division, 2001) pp.8-9, Quoted in Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Intergration and Electronic Commerce*':p21

The Internet first became available in Kenya during 1993. Full Internet access was established in 1995. The African Regional Centre for Computing (ARCC), an NGO based in Nairobi, Kenya, became the first provider of web-based Internet service. The first commercial ISP (Internet Service provider), Formnet began operating in 1995. Soon competition increased with the entry of three other ISPs. All the ISPs would lease analogue or digital data lines from Kenya to the US to access the Internet backbone.[17]

In 2000, there were about 200,000 Internet users in Kenya, with an estimated monthly growth of 300 new subscribers each month. Internet usage in Kenya has increased over time from a partly 0.7% of the population (200,000 users) in 2000 to 24.4% of the population (10,492,785 users) in 2011. Kenya is ranked fourth among Africa's top internet countries as at December 31 2011 figures. Nigeria is ranked the number one country with 45 million users but this is attributed to its huge population of over 155 million people. [18] This growth in internet penetration is significant but not sufficient.

In Kenya, commercial banks have continued to embrace the use of the Internet as a remote delivery channel for banking services. As at 31st December 2011 twenty three banks were offering various internet products to their customers. Internet services provided include; opening accounts, transferring funds to different accounts, online

[17] The Kenya Internet World Stats, Usage and Population Statistics. <http ://www. *internetworldstats .com /stats.htm.*> Accessed on 08/09/2012.
[18] ibid

viewing of the accounts, online inquiries and requests, online salaries payments, clearing cheques status query and instant alerts or messages of account status.[19]

While internet banking is a fast and convenient mode of conducting banking transactions, it is yet to gain acceptance among banking customers due to fears and apprehension in this mode of banking. The banks that have adopted the product have been faced with various problems ranging from security concerns by the users, lack of adequate legal framework, poor marketing strategies and issues regarding the connectivity to the internet banking site.[20]

Banking customers will feel more comfortable using new electronic services, if they are aware of a defined legal framework that would allow them to identify their rights and obligations with the least possible uncertainties.[21]There is no specific law that deals with internet banking in Kenya. The Constitution and various Acts of parliament capture different aspects of the law. The law applies generally without specific reference to electronic banking or internet banking. The applicable banking laws are antiquated and were passed several decades ago and are no longer suitable to deal with the legal issues associated with internet banking and has reached their limits of flexibility and time has come for such laws to be updated to the age of widespread electronic banking.[22] This does not necessarily mean that a fundamental overhaul of banking laws is needed, instead

---

[19] Bank Supervision Annual Report 2011: p 25, prepared by the Central Bank of Kenya < http:// www. centralbank.go.ke.> Accessed on 08/09/2012.

[20] Gaitungu, David N., "Analysis of the challenges facing Internet banking in Kenya: A case of Commercial Bank of Africa Ltd." (2012). Accessed from http://ir-library.ku.ac.ke.

[21] Mohammed Y Alem, "E- Banking and other Financial Services: Regulatory Development in selected Arab Countries": 3 <http://scribd.com/doc/66510348/E-banking-and- Other- Financial-Services-Regulatory-Developments-in-Selected-Arab- Countries.> Accessed:10/6/2012.

[22] Kethi D. Kilonzo, "An Analysis of the Legal Challenges posed by Electronic Banking," Kenya Law Review 1 (2007) : 323 <www.kenyalaw.org/Downloads.../Kilonzo_electronic_banking.pdf > Accessed:29.06.2011

discreet changes are required to address the specific issues presented by electronic banking and therefore put it on an equal plane with traditional banking.[23]

Several efforts have been made to modernise banking laws in line with developments in electronic banking occurring in the industry. In the Budget speech for fiscal year 2004/2005, the Minister for Finance proposed to table the National Payments System and Electronic Funds Transfer Bills in Parliament. The National Payment Systems Act was passed in 2011 but the EFT Bill is yet to become law.[24] The CBK and the Ministry of Finance have also collaborated in drafting the e-Transactions Bill that seeks to facilitate and promote the use of electronic transactions in Kenya by creating legal certainty and public trust around transactions which are conducted with various forms of information and communications technologies.[25] These are critical Bills that address the new challenges facing the banking industry but until they are enacted they remain mare proposals.

This paper calls for passage of legislation tailored to meet the new legal challenges that arise out of adoption of internet banking in the industry.

1.1 Problem Statement

From the perspective of banking products and services being offered through internet, internet banking is nothing more than traditional banking services delivered through an electronic communication backbone, through the internet. But in the process it has thrown open issues which have ramifications beyond what a new delivery channel would

---

[23] ibid

[24] CBK Annual Report 2005, pg 70, < http:// www.centralbank.go.ke>Accessed: 10/09/2012.

[25] CBK Annual Report 2008 pg55, < http:// www.centralbank.go.ke>Accessed: 10/09/2012.

normally envisage and hence has compelled regulators world over to take note of this emerging channel. [26]

Some of the distinctive features of internet banking are:

1. It removes the traditional geographical barriers as it could reach out to customers of different countries. This has raised the question of jurisdiction of law / supervisory system, to which such transactions should be subjected.
2. It has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges.
3. Security of banking transactions, validity of electronic contract and customers' privacy have assumed different dimensions given that internet is a public domain, not subject to control by any single authority or group of users and
4. It poses a strategic risk of loss of business to those banks who do not respond in time to this new technology, being the efficient and cost effective delivery mechanism of banking services.

The regulatory and supervisory concerns in internet banking arise mainly out of the distinctive features outlined above. These concerns can be broadly addressed under three broad categories: [27]

(i) Legal and regulatory issues;

(ii) Security and technology issues and

(iii) Supervisory and operational issues.

---

[26] Shri S. R Mittal& others, "Report on Internet Banking", Working Group set up by Reserve Bank of India, June 2001:2-3<http://www.rbi.org.in/scripts/PublicationsReportDetails.aspx.> Accessed 5/09/2012.

[27] Ibid. p2

Legal issues cover those relating to the jurisdiction of law, validity of electronic contract including the question of repudiation, gaps in the legal / regulatory environment for electronic commerce.

Security of internet banking transactions is one of the most important areas of concerns to the regulators. Security issues include questions of adopting internationally accepted state of-the art minimum technology standards for access control, encryption / decryption, firewalls, verification of digital signature, Public Key Infrastructure (PKI) etc. The regulator is equally concerned about the security policy for the banking industry, security awareness and education.[28]

The supervisory and operational issues include risk control measures, advance warning system, information technology audit and re-engineering of operational procedures. The regulator would also be concerned with whether the nature of products and services offered are within the regulatory framework and whether the transactions do not camouflage money laundering operations.[29]

The world over, central bankers and regulators have been addressing themselves to meet the new challenges thrown open by this form of banking. The thrust of regulatory thinking has been to ensure that while the banks remain efficient and cost effective, they must be aware of the risks involved and have proper built-in safeguards, machinery and systems to manage the emerging risks. This can only be done guided by an appropriate legal and regulatory framework to address the above legal and regulatory issues associated with internet banking.[30] The central question for legal practitioners and lawmakers revolves around how to accommodate the use of new technology in banking

[28] Ibid
[29] Ibid
[30] Ibid, p 3.

and financial services in the already existing law and how to regulate it from a concrete and clear legal perspective.[31] As discussed, there is no specific law that deals with internet banking in Kenya. The Constitution and various Acts of Parliament capture different aspects of the law. The law applies generally without specific reference to electronic banking or internet banking. Accordingly, any legal and regulatory framework to govern internet banking should at the minimum revolve around the setting, enactment and enforcement of a set of laws comprising:

a) Law on Electronic and Digital Signature

b) Law or Regulation on third-party Certification Authorities

c) Laws or Regulations on e-Banking per se

d) Law on Data Privacy

e) Laws on Anti-Money Laundering.[32]

The above set of laws will act as a benchmark when examining the current legal and regulatory framework governing internet banking in Kenya with a view of identifying the gaps and the legislative and regulatory reforms that are necessary to bring it at par with international best practices in other jurisdictions.

1.2 Research Objectives

The main objective of this paper is to examine the current legal and regulatory framework governing internet banking in Kenya.

---

[31] Mohammed Y Alem, "E- Banking and other Financial Services: Regulatory Development in selected Arab Countries": 3 <http://scribd.com/doc/66510348/E-banking-and- Other- Financial-Services-Regulatory-Developments-in-Selected-Arab- Countries.> Accessed:10/6/2012.

[32] ibid

Specifically, the paper identifies the international best practices on internet banking and points out specific shortfalls in the legislative and regulatory framework in Kenya that makes it inadequate to address legal issues associated with internet banking.

Finally, the paper outlines its findings, conclusions and makes recommendations on the legislative and regulatory reforms that are necessary in order to bring Kenya's legal and regulatory framework on internet banking at par with the best practices in the other jurisdictions.

1.3 Research Questions

The study answers the following research questions:

1. What is the current legal and regulatory framework for internet banking in Kenya?
2. Is the current legal and regulatory framework adequate to regulate internet banking in Kenya?
3. What legislative and regulatory reforms are necessary in order to bring Kenya's legal and regulatory framework on internet banking at par with the best practices in other jurisdictions?

1.4 Hypotheses

The current legal and regulatory framework in Kenya is inadequate to address the legal issues associated with internet banking and is therefore in need for reform. The study is based on the following assumptions:-

1. The current legal framework is inadequate to deal with the legal issues that arise with the adoption of internet banking in Kenya.

2. There is need to improve and strengthen the legal and regulatory framework in light of comparable developments in the law that have occurred in other jurisdictions.
3. Adoption of internet banking aggravates some of the traditional banking risks creating unique challenges to regulators and bank supervisors.

1.5 Justification of the Study

The banking industry in Kenya has witnessed tremendous changes linked with the developments in information communication technology (ICT) over the years. The quest for survival, global relevance, maintenance of existing market share and sustainable development has made exploitation of ICT through the use of automated devices imperative in the industry. Application of ICT concepts, techniques and the development of policies and strategies has become a subject of fundamental importance and concern to all banks and indeed is a prerequisite for local and global competitiveness. ICT has continued to change the way banks and their corporate relationships are organized locally and worldwide.[33]

However, developments in ICT bring with them certain risks which require to be mitigated appropriately. Therefore with regard to ICT driven products, the oversight responsibility and management has been placed on the board of directors and senior management of the financial institutions to put in place appropriate and adequate controls in order to provide customer confidence on confidentiality, integrity and timely

[33] CBK, Supervision Annual Report 2010(Chap 2):p 6 <http:// www.centralbank.go.ke.> Accessed on 8/09/2012

availability of banking services. What is the role of the law in regulation and supervision of ICT driven products such as Internet banking?

Scholars in this area have emphasized more on the factors affecting adoption of Internet banking from a customer's or banker's perspective. Sara Naima Baraghani investigates customers' adoption of internet banking in Iran.[34] The study shows that, attitude; perceived behavioral control, perceived usefulness, and perceived ease of use and trust significantly influence customers' intention toward adopting internet banking. Ravi Nath, Paul Schrick and Monica Parzinger concentrate on the bankers' perspectives on Internet banking emphasizing more on strategic considerations such as reduction of transactions costs, increase of customer base and improving cross-selling opportunities as major considerations by banks in adopting e banking technologies.[35]

This thesis seeks to shift the attention from customers' and bankers' perspectives of adoption of e-banking technologies to consideration of the adequacy of the legal and regulatory infrastructure that underpins the rolling out these ICT based services.

The study will enrich the existing jurisprudence on internet banking in Kenya and the market regulator, bank managers and other decision makers in the banking sector would find the suggested recommendations useful in reforming the laws governing the industry

Finally, internet banking is a relatively new ICT based delivery module that is being adopted by commercial banks in Kenya and so it is worthwhile to conduct this study, whose result could be used to improve the banking sector, and enhance the quality of internet banking services in Kenya.

---

[34] Sara Naimi Baraghani, *"Factors that Influence Adoption of Internet Banking"* (Msc..diss, Lutea University of Technology,(2007), 1.<http://www. pure.itu.se/.../LTU-PX-EX-08099_SE.pdf> Accessed: 9.09.2011.

[35] Ravi Nath, Paul Schrick and Monica Parzinger, "Bankers' Perspectives on Internet Banking: pp21-22.

1.6 Theoretical Framework.

The study reviews and builds up on the concept of the internet, bank and banking There are two broad traditions with respect to the economic theories of regulation. public interest theories of regulation and private interest theories of regulation. The first tradition assumes that regulators have sufficient information and enforcement powers to effectively promote the public interest. This tradition also assumes that regulators are benevolent and aim to pursue the public interest. According to these theories, the regulation of firms or other economic actors contributes to the promotion of the public interest. This public interest can further be described as the best possible allocation of scarce resources for individual and collective goods and services in society. In theory, it can even be demonstrated that, under certain circumstances, the allocation of resources by means of the market mechanism is optimal. [36]

Because these conditions do frequently not apply in practice, the allocation of resources is not optimal from a theoretical perspective and a quest for methods of improving the resource allocation arises.[37] This situation is described as a market failure. A market failure is a situation where scarce resources are not put to their highest valued uses. One of the methods of achieving efficiency in the allocation of resources when a market failure is identified is government regulation.[38] Prudential banking regulations fall under

---

[36] Arrow, Kenneth J. (1985), 'The Potentials and Limits of the Market in Resource Allocation', in Feiwel, G.R. (ed.), Issues in Contempory Microeconomics and Welfare, London, The Macmillan Press, 107-124. .As quoted in Johan Den Hertog, "Review of Economic Theories of Regulations", Tjalling C Koopmans Research Institute, Discussion Paper Series 10-18.Utrecht School of Economics, Utrecht University,December 2010, 5<http://www.koopmansinstitute.uu.nl Assessed on 3.12.12

[37] Bator, Francis M. (1958), 'The Anatomy of Market Failure', 72 Quarterly Journal of Economics, 351-379. .As quoted in Johan Den Hertog, "Review of Economic Theories of Regulations", Tjalling C Koopmans Research Institute, Discussion Paper Series 10-18.Utrecht School of Economics, Utrecht University,December 2010, 5<http://www.koopmansinstitute.uu.nl Assessed on 3.12.12

[38] ibid

Public interest theory. The Government through its specially administrative agencies is entrusted with the task of regulating and overseeing the orderly functioning of the financial markets. The concept of regulation refers broadly to the creation of formal standards and codes of conduct which private individuals and firms must follow.[39] Legislation is the ultimate source of regulation. The government will ensure that the rules are followed through persuasion and formal enforcement by means of administrative and criminal penalties.

Principal economic rationales for financial regulation include;[40]

1. Prudential supervision to institutions especially banks to ensure they are soundly capitalised and correspondingly less vulnerable to "runs" and other market shocks to prevent market failure (Systemic risks).[41]
2. Information asymmetry between the banks and their customers, which make it difficult for the customers to assess the risks and returns of the transaction they undertake. Justification for regulations is clearly strongest for measures to improve disclosure of information on one hand and improve the ability customers have to understand the implications of that disclosure on the other. This would lessen the difficulty customers have in assessing the prudential soundness of the firm with which they deal.

Economic regulation refers to restrictions on prices, interest, quantity of production, entry in and out of the industry.[42] For example rules that prohibit all persons from providing banking services unless the competent authority grants a special license to regulate the

---

[39] Henry Thorton, "Why Regulate," Lecture City University Business School, (4th November 1998) <http://fsa.gov.uk./library/communication/speeches/1998/sp19.shtml> Accessed: 10.07.2012.

[40] Ibid

[41] The bank sits at the centre of the payment system and the failure of one bank, even if attributable to management incompetence, can bring about domino effects on others. There is a case in certain circumstances, for rescuing a failing institution since the combined result of bank failure, which may include the loss of solvent, profitable banks, justifies holding up the first domino.

[42] Supra note 39,p4

entry of market participants in the banking industry. Social regulations seek to correct some form of market imperfections or failure. Environmental, public health and safety regulations fall into this category. Example includes disclosure of information regarding risks associated with services provided.

Public interest theories usually assume that regulation aims to establish economic efficiency. Interpreted in this way, these theories are unable to explain why on occasion other objectives such as procedural fairness or redistribution are aimed for at the expense of economic efficiency.[43]

Another tradition in the economic studies of regulation proceeds from different assumptions. Regulators do not have sufficient information with respect to cost, demand, quality and other dimensions of firm behavior. They can therefore only imperfectly, if at all, promote the public interest when controlling firms or societal activities. It is generally assumed that all economic agents pursue their own interest, which may or may not include elements of the public interest. The differences in objectives of economic agents and the costs involved in the interaction between them may effectively make it possible for some of the agents to pursue their own interests, perhaps at the cost of the public interest. Economic theories that proceed from these latter assumptions are therefore often called *'private interest theories of regulation'*.[44]

The capture theory assumes that in the course of time, regulation will come to serve the interests of the industry involved. According to these theories, capture is the result of the

[43] Joskow,Paul L. and Noll, Roger C. (1981), 'Regulation in Theory and Practice: An Overview', in Fromm, Gary (ed.), Studies in Public Regulation, Cambridge, MA, The MIT Press, 36.

[44] Johan Den Hertog, "Review of Economic Theories of Regulations", Tjalling C Koopmans Research Institute, Discussion Paper Series 10-18.Utrecht School of Economics, Utrecht University,December 2010, 5

increasing power of the agency which arises because the agency in its ongoing relationship gets to know the firm better and better. The agency has thus more and more opportunities to pursue its own objective and the political principal can only control this by having more stringent administrative rules and fair and open procedures. This limitations 'cripple' the agency and makes it receptive for the influences of the regulated firm. In the course of time, other political priorities arrive on the agenda and the monitoring of the regulatory agency by legislators is relaxed. This leads in time to the regulatory agency coming to represent the interests of the branch involved. For an overview of the various strategies available to be applied by agencies and regulated companies.[45]

The capture theory is unsatisfactory in a number of respects. Firstly, there is insufficient distinction from the public interest theory, because the capture theory also assumes that the public interest underlies the start of regulation. Secondly, it is not clear why an industry succeeds in subjecting an agency to its interests but cannot prevent its coming into existence. Thirdly, regulation often appears to serve the interests of groups of consumers rather than the interests of the industry. Regulated companies are often obliged to extend their services beyond voluntarily chosen level of service. Examples are transport services, the supply of gas, water and electricity and telecommunication services to consumers living in widely scattered geographical locations. Fourthly, much regulation, such as environmental regulation, regulation of product safety and labor conditions are opposed by companies because of the negative effect on profitability. Finally, the capture theory is more of a hypothesis that lacks theoretical foundations. It does not explain why an industry is able to 'take over' a regulatory agency and why, for

[45] Ibid,p22-23

example, consumer groups fail to prevent this takeover. Nor does it explain why the interaction between the firm and the agency is characterized by capture instead of by bargaining. Recently dynamic capture theories have been developed, explaining the life-cycle of regulatory agencies evolving over time from acting in the public interest to becoming increasingly inefficient and more eager to please private interests.[46] business, the bank-customer relationship, e-banking, e-finance, e-commerce and international banking.

1.7 Conceptual framework

1.7.1 The Internet

Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (often called TCP/IP) to serve million of users world wide. Openly accessible and globally connected computers enable the two-way transportation of information between bank and the customer.[47]

The basic function of the Internet Protocol (IP)[48] is to receive and transmit any information which may take digital form. The primary Internet code enables the transmission of data from one computer to another without being necessary that the originator and recipient of information share a direct network connection. Although individual computers may be connected to the network or disconnected, at the will of their administrators or because of disruptive events, data transmitted over the internet always discovers open network routes through the remainder of available networks and servers. As a result the internet enables the unimpeded circulation of data, which may be

---

[46] ibid

[47] Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Integration and Electronic Commerce*' (Cambridge University Press, 2006), p9

[48] The Internet Protocol is the method or code by which data is sent from one computer to another on the Internet.

retrieved by or transmitted to computers located anywhere in the world without the process being affected by the territorial proximity or lack thereof, between the originator and the final receipient of the data.[49]

The internet was originally intended for research, not regulated commercial and financial activities, therefore its technical specifications reflect the conscious decision to disable control and stimulate speed and efficiency in the circulation of digital data. For that reason, users and financial institutions impose control of access or content peripherally, without the core Internet Protocol being otherwise affected. Banking lies at the heart of the tension between 'free flow of data' and 'control in paradoxical way.[50]

In the context of banker-customer relationship, data transmitted from the bank to the customer and vice versa may result in the establishment, alteration, exercise or termination of legal rights and obligations in accordance with the contract between the bank and customer. In that respect, the internet enables the initial establishment of the banker-customer relationship and electronic delivery and performance of services thereafter, within the boundaries set by available technical and legal mechanisms of authorisation and access control.[51]

1.7.2 Bank and Banking Business

Section 2 of the Banking Act[52] defines a bank as a company which carries on or proposes to carry on banking business in Kenya but does not include the Central Bank.

The Banking Act[53]defines banking business as:

---

[49] Preston Gralla, *How the Internet Work* (Indianapolis: Que, 2004), ch1. Quoted in Apostolos Ath. Gkoutzinis, 'Internet Banking and the Law in Europe':p9.
[50] Ibid. p18.
[51] Ibid. p 9.
[52] Cap 488 Laws of Kenya. An Act of Parliament to amend and consolidate the law regulating the business of banking in Kenya and for connected purposes.

"The accepting from members of the public of money on deposit repayable on demand or at the expiry of a fixed period or after notice; the accepting from members of the public of money on current account and payment on and acceptance of cheques; and the employing of money held on deposit or on current account, or any part of the money, by lending, investment or in any other manner for the account and at the risk of the person so employing the money."

The statutory definition of a bank given above adopts a monetary dimension with emphasis on the financial nature of business that such a company would conduct.

In the *United Dominions Trust Case*[54] Lord Denning defined a bank as follows:

"……An establishment for the custody of money received from, or on behalf of, its customers. Its essential duty is to pay their drafts on it: its profits arise from the use of money left unemployed by them…." [Emphasis added]

Lord Denning enables one to appreciate the fact that banks can and often do invest and conduct transactions using their client's funds. Therefore banking business is not restricted to the customer's use of the funds only.

1.7.3 The banker-customer relationship

The relationship between the online bank and customer is based on contract. It consists of general contract which comes into being upon the establishment of the customer-banker relationship, and the special contracts, which arise only by specific agreement of the parties.[55]

The bank account is the foundation of separate foundation of separate and distinct contract that come into being during the life of the banker- customer relationship. The

---

[53] Under Section 2(1).
[54] (1966) 1 All ER, p. 968.
[55] Apostolos Ath. Gkoutzinis, 'Internet Banking and the Law in Europe':p9.

bank accepts the customer's deposits made either by the customer or a third party by means of collection from another bank account and repay a sum of equivalent value in total or in part on demand or at a specified date, with or without interest, to the customer or to a third party at the customer's order.[56]

In English law, the operation of a current account in which sums of money are from time to time paid in or withdrawn by the customer is an essential element of the business of banking. The facilities afforded to the account holder for deposit of funds and making account based payments lie at the heart of the legal relationship. It was established in *Foley v Hill* [57] that between the bank and customer the current account establishes a relationship of debtor and creditor. All money coming to the banker's hand for credit into a bank account is to be taken as lent to the banker who in turn undertakes to repay the equivalent sums of money subject to additional obligations and limitations related to practicability of the banking practice.

In Kenya, acceptance of deposit by way of business constitutes *regulated activity.* Section 3(1) (a) of the Banking Act, states that:

"No person shall in Kenya, transact any banking business or financial business or the business of a mortgage finance company unless it is an institution or a duly approved agency conducting banking business on behalf of an institution which holds a valid licence."

The use of the internet as an alternative means of initiating and transmission of customer instructions to the customer's bank for the performance of electronic transfer of funds (EFT) is one of the most visible aspects of internet banking. EFT initiated via the Internet

---

[56] See generally *Joachimson v. Swiss Bank Corpn* [1921] 3KB 110.
[57] (1848) 2 HL Cas 28.

encompasses any type of payment order initiated through electronic device, telephonic instrument or computer or magnetic tape so as to order, instruct or authorise a financial institution to debit and credit an account.

1.7.4 E-commerce

Electronic commerce (E-commerce) is the sharing of business information, maintaining business relationships, and conducting business transactions by means of telecommunications networks. In today's business environment, where the operational boundaries between firms have become fluid, it is often both pragmatically and analytically unfruitful to separate interorganizational and intraorganizational business processes. Therefore, as understood here, E-commerce includes the sell-buy relationships and transactions between companies, as well as the corporate processes that support the commerce within individual firms.[58]

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.[59]

1.7.5 E- banking

Electronic banking can be defined as the provision of banking services and the initiation and performance of payments through the banking systems by electronic means and other advanced technologies. Electronic banking is a conceptually generic term, which denotes

---

[8] Vladimir Zwass, 'Electronic Commerce: Structures and Issues', International Journal of Electronic Commerce vol1, No 1(1996),p2,< http://www.jstor.org/stable/27750797>Accessed 8.09.2011

[9] Kethi D. Kilonzo, "An Analysis of the Legal Challenges posed by Electronic Banking," Kenya Law Review 1 (2007) : 325

banking services provided through a variety of access devices and links of communication.[60] Internet banking refers to the provision of electronic banking services via the internet, commonly through a personal computer (PC) or other access device with Internet capabilities.[61] Internet banking gives the customers the ability to access virtually any type of banking services (except cash) in any place and at any time.[62]

1.7.6 E- finance

The concept of e-finance may broadly be defined as the provision of financial services using information technology, telecommunications and computer networks. Internet banking is a sub set of e- finance[63]since it is constitutes provision of electronic banking services via the internet.

1.7.7 International Banking

International banking is the process in which financial institutions allow foreign clients to access and use their services. It therefore means that between the bank, the customer and the payee at least two of them are separated by an internationally recognised border.[64] Internet banking grants the opportunity to use computer networks to provide banking services via the internet across national borders. Internet acts as a catalyst of international financial integration. Cross border Internet banking presents new range of risks. Unless these issues are fully understood and financial institutions and customers are assured that the departure from the familiar local markets will not be penalized by unacceptable levels

---

[60] Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Integration and Electronic Commerce*', p7.
[61] Ibid,p8
[62] ibid
[63] Ibid, p7
[64] Gkoutzinis, 'Internet Banking and the Law in Europe' : p 19

of legal risks, the prospects of using the Internet as a means of engaging in financial activities across borders are unpromising.[65]

1.8 Literature Review.

Though information on the subject of e-banking abounds the internet, there are scanty scholarly texts on the subject. The texts become even fewer when you consider the adequacy of the legal and regulatory framework governing internet banking in Kenya. To that extent there is a lot of latitude to build up jurisprudence in this area.

However, a review of the texts and articles consulted is given below:

Books/texts

Apostolos Ath. Gkoutzinis in his book Internet Banking and the Law in Europe[66] focuses on services provided via the internet by commercial banks and explore the potential contribution of electronic finance to meeting the objectives of financial integration in a single European market. In chapter one, the reader is introduced to the basic concepts and services relating to electronic finance and internet banking. Electronic finance is the provision of financial services and creation of financial markets using information technology, telecommunications and computer networks. Internet is seen as a catalyst of international financial integration in this era of liberalization of international trade in financial services in global and regional economic cooperation. The Chapter discusses the internet and banker-customer relationship, e-commerce and international financial integration. The Internet eradicates the constraints of geography and distance in the movement of digital data. In chapter two, the author examines the legal concepts and

[65] Ibid.

[66] Apostolos Ath. Gkoutzinis, '*Internet Banking and the Law in Europe : Regulation, Financial Integration and Electronic Commerce*' (Cambridge University Press, 2006), pp 1-318.

foundations of electronic banking activities in three countries examined namely United Kingdom, France and Germany. The European Union has made great strides in coming up with an adequate legal framework to underpin internet banking through passing directives such as e-signature and data privacy. Countries such as the UK have recently reviewed their laws governing the business of banking to bring it in line with e-banking developments. However the proceeding chapters of this book discuss cross border internet banking and convergence of laws in the single European market which is outside the scope of this thesis. The thesis focuses on the domestic legal infrastructure as opposed to the cross border legal framework.

Michael Brindle and Raymond Cox[67] in chapter 5 of Law of Bank Payments, comprehensively discuss internet payment methods. The author looks at the conflict of law and jurisdictional issues that arise when payments are made over the internet in performance of a payment obligation concluded over the internet. This can raise issues such as validity of the contract entered by electronic means.. This puts to the fore the terms and conditions that are set out in the internet agreements or contracts that are entered by the parties to an internet transaction. The contract should deal with the issues of proper law and jurisdiction to remove uncertainty in case a dispute arises. The chapter also considers the role of encryption, electronic signatures and trusted third parties. The author discusses key issues that affect internet payment methods such as authentication and non- repudiation (whether the payment message originates from, and will it bind the person who purports to have sent it). Is the message forgery proof and is the customer's

[67] Michael Brindle And Raymond Cox,(eds), '*Law of Bank Payments*', 3 eds, (Thomson Sweet and Maxwell), pp 255-321.

confidential information protected from unauthorized third parties. The book discusses how these issues are dealt with by the English legal system and the European Union legal systems contrasting it with the position in the United States. The text will be useful as a reference point when discussing international best practices in internet banking. The author questions whether the existing body of law referable to those payment system can be applied and to what extent it needs to be adapted or an entirely new legal framework created.

Chapter 4 of Paget's Law of Banking discusses Money laundering legislations in the United Kingdom.[68] The chapter discusses various legal instruments such as Council Directive 91/308/EEC on the Prevention of the use of the financial system for the Purpose of Money Laundering made pursuant to arts 47 and 95 of the Treaty of Rome. It argues that the effectiveness of the efforts to eliminate money laundering is depended on harmonisation of national implementing measures by ensuring that money laundering is prohibited. This can only be done by passing an anti-money laundering legislation. It requires the member states to prevent anonymity in banking transaction by maintaining records and reporting suspicious transaction. This text can be contrasted with our Proceeds of Crime and Anti- Money Laundering Act 2009 to ascertain the gaps in this new legislation. The chapter looks at equivalent provisions in the Financial Services Markets Act (FSMA) 2000 on reduction of financial crimes, The Drug Trafficking Act 1994 on retaining proceeds the proceeds of drug trafficking, The Criminal Justice Act 1988 on retention of proceeds of criminal conduct and money laundering. The Kenyan position is well articulated by George Kegoro in the book titled Tackling Money

[68] Mark Hapgood Qc,Paget Law of Banking,12 edn: Butterworths,pp83-99

Laundering in East and Southern Africa.[69] He argues that the war on money laundering should be fought from two levels, measures to detect and punish economic crime which generates the money that then needs to be laundering and measures needed to address problems of money laundering directly. The anonymous nature of internet banking and the lack of contact with bank employees may be misused for money laundering.

Reports

In the year 2000, the Reserve Bank of India constituted a working group to examine different issues relating to internet banking and make recommendations on the technological, security, legal and operational standards that should be adopted in India based on the international best practices.[70] The report is exhaustive and outlines the salient features of internet banking and examines different aspects of Internet banking from regulatory and supervisory perspective and recommends appropriate standards for adoption in India, particularly with reference to the following:

1. Risks to the organization and banking system, associated with Internet banking and methods of adopting International best practices for managing such risks.
2. Identifying gaps in supervisory and legal framework with reference to the existing banking and financial regulations, IT regulations, tax laws, depositor protection, consumer protection, criminal laws, money laundering and other cross border issues and suggesting improvements in them.
3. Identifying international best practices on operational and internal control issues, and suggesting suitable ways for adopting the same in India.

---

[69] George Kegoro, The Control of Money Laundering and Terrorist Funding in Kenya,, Chap 3,pp3875

[70] Shri S. R Mittal& others, 'Report on Internet Banking', Working Group set up by Reserve Bank of India, 2001:pp1-130 <http://www.rbi.org.in/scripts/PublicationsReportDetails.aspx.> Accessed 5/09/2012.

4. Recommending minimum technology and security standards, in conformity with international standards and addressing issues like system vulnerability, digital signature ,information system audit etc.

5. Clearing and settlement arrangement for electronic banking and electronic money transfer; linkages between internet-banking and e-commerce

This report was crucial in narrowing down the legal and regulatory issues that affect internet banking in any legal framework. The report was of high probative value since the committee was composed of experts in the fields of banking regulation, commercial banking, law and technology. The legal framework in India is comparable to that of Kenya therefore there is a higher likelihood that Kenya faces similar challenges in buttressing the legal framework governing internet banking and any reforms already implemented in India would easily be replicated in Kenya.

Central Bank reports both Annual reports and Bank supervision annual report have been useful sources of data in this thesis. The section dealing with banking sector reforms is crucial in stating the state of the banking sector giving information as the number of banks operating in the country and their performance. The report must have a section summarizing the developments occurring in the national payment systems. Regional integration developments must have the regional initiatives being conducted to prevent money laundering among other issues such as financial sector integration efforts across the continent. Efforts are being made to have one monetary system in the East African Community (EAC) and in the continent in line with globalization and trade liberalization. ICT banking products such as internet banking would act as a catalyst to integration of

the various systems due to its ability to transact in this medium across national borders. The Supervision reports usually have sections outlining various developments in the local banking industry especially on information technology, recent changes in banking laws and regulations, prudential guidelines, current supervisory issues and developments in banking supervision.

These reports have been crucial in getting the most current and historical developments on the nature of the banking sector, legal and supervisory issues and any changes in the legal and regulatory framework governing the industry.

The Basel Committee on Banking Supervision issued risk management principles for electronic banking in May 2001.[71] The Risk Management Principles fall into three broad, and often overlapping, categories of issues: Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management. The Committee has expressed supervisory expectations and guidance in the form of Risk Management Principles in order to promote safety and soundness for e-banking activities, while preserving the necessary flexibility in implementation that derives in part from the speed of change in this area. Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk are also present in internet banking. These risks get intensified due to the very nature of Internet banking on account of use of electronic channels as well as absence of geographical limits.

Risk taking is an inherent element in banking and profits are in part rewards for successful risk taking in business. On the other hand, excessive, poorly managed risks

---

[71] Available on the Bank for International Settlements' website at http://www.bis.org.

can lead to loses and thus endanger the safety of banks deposits. Such actions could compromise the bank's ability to meet its business objective. It is imperative that a risk management forms part of the legal framework to ensure that the managers of financial institutions take only the risks that are warranted. The legal framework must be flexible in order to keep pace with the changes in technology in the industry.

Articles and electronic journals

Kethi Kilonzo[72] analyses the legal challenges posed by electronic banking. She equates electronic banking to electronic funds transfer (EFT). Electronic banking is a generic term to a number of electronic transactions that are provided through a variety of access devices and other advanced technologies and includes but not limited to electronic funds transfer. The author links concepts of e-banking and e-commerce and argues that the two complement each other with e- banking acting as the payment mechanism for e-commerce. She discusses digital signatures, documentation of EFT and unauthorised transfers and argues that these areas remain unregulated in Kenya. There is a legal vacuum as far as e-banking in Kenya is concerned and there is no specific law governing electronic commerce or electronic payments in Kenya. The applicable banking laws are antiquated and banks are aware of this vacuum and rely on the clausal terms in the contract they enter with customers to exempt them from liability in case of fraud, malfunctions in electronic payment systems. The article was written in 2007 before the Kenya Information Communication Act was amended in 2009 to provide provisions to regulate e- transactions and e- commerce. The author calls for regular review and amendment of the existing law to fit existing social, economic and political environment.

---

[72] Kethi D. Kilonzo, "An Analysis of the Legal Challenges posed by Electronic Banking," Kenya Law Review 1 (2007) : 323 <www.kenyalaw.org/Downloads.../Kilonzo_electronic_banking.pdf > Accessed:29.06.2011

Consumer protection laws would rein on the banks and protect the customer from the unequal bargaining power that favours the bank to the detriment of the customer in the banker- customer relationship.

Ravi Nath, Paul Schrick and Monica Parzinger[73] examine bankers' views on providing banking services to customers using the web. The paper draws nexus between e-commerce and e-banking. The number of firms that buy and sell over the internet have increased and the revenue that is generated by e-commerce is growing at an exponential rate. Bankers see internet banking as a strategic opportunity that can reduce transaction costs, enhance customer service, increase the customer base and improve cross-selling opportunities. Sara Naima Baraghani investigates customers' adoption of internet banking in Iran.[74] The study shows that, attitude; perceived behavioral control, perceived usefulness, and perceived ease of use and trust significantly influence customers' intention toward adopting internet banking. The paper only discusses the benefits of internet banking to the bank and customer but does not discuss the role of law in regulating internet banking. The two papers only discuss the benefits of internet banking to the banker and customer but do not discuss the role of the law in regulating internet banking It does not enumerate he legal issues that arise with the adoption of internet banking. The subject matter of this thesis (adequacy of the legal framework in dealing with issues arising from internet banking) has not been discussed by the authors of the article and thesis at all

---

[73] Nath, Paul Schrick and Monica Parzinger, 'Bankers' Perspectives on Internet Banking':21-36

[74] Sara Naimi Baraghani, *"Factors that Influence Adoption of Internet Banking*" (Msc..diss, Lutea University of Technology,(2007), 1.<http://www. pure.itu.se/…/LTU-PX-EX-08099_SE.pdf> Accessed: 9.09.2011.

Andrea Schaechter[75] provides an overview of issues in electronic banking. The author states that the dependence on technology for providing banking services with the necessary security, and cross border nature of the transactions, involves additional risks for banks and the new challenges for banking regulators and supervisors. This paper discusses issues such as, authorization or licensing of virtual banks; cross-border issues such as offshore banking; risk management of operational, reputational and legal risks; money laundering; consumer protection and education and how those issues are currently being addressed by regulatory and supervisory authorities. This article shifts the attention from the customer and banker to the bank regulators and supervisors and how they are dealing with the various challenges brought by internet banking.

Tamara Dinev and Paul Hart[76]examine the relationships between two dimensions of privacy concerns.(Example, concerns related to finding personal information on the internet and concerns related to the possible abuse of personal information submitted online) and the intended e-services use at each level of information exchange. Privacy concerns increase as the amount and sensitivity of personal information submitted through Web sites increases. This phenomenon, in turn, has fueled concerns about user vulnerability related to information and personal privacy. Online activities and transactions generate detailed electronic footprints that expose individuals' preferences, interests, and behaviors even if the user has never submitted specific personal identifiable

[75] Andrea Schaechter, " Issues In Electronic Banking: An Overview, IMF Policy Discussion, PDP/02/6, 2002, 1- 26< www.imf.org/external/pubs/ft/pdp/2002/pdp06.pdf > Accessed:8.09.2011

[76] Tamara Dinev and Paul Hart, 'Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use', e-Service Journal, Vol. 4, No. 3 (Summer 2006), pp. 25-60 < www.muse.jhu.edu/journals/eservice_journal/v004/4.3dinev.html>Accessed:10/6/2011

information. Thus, the Internet provides an unprecedented means to unobtrusively observe user Internet activity and to gather copious amounts of information about individuals and their transactions for both government and private sector purposes. This calls for enactment of legislation on data privacy to determine the manner in which personal information is to be dealt with.

Ersida Teliti and Rezarta Mersini[77] in their assessment of e-banking services and legal framework in Albania argue that the impact of e-banking is not limited to industrially powerful and developed economies. Transition economies in developing countries prone to underdeveloped banking systems have been witnesses to the advantages of e-banking. Developing countries have an advantage because they can learn from the advanced economies in terms of implementing internet technologies in banking services. E-finance can be introduced quickly in developing countries even where the basic financial infrastructure is weak. Kenya is a developing nation and has embraced internet banking despite the weak legal framework that governs e- banking. Kenya can emulate and learn from the developed countries especially European countries that have successfully implemented internet banking in their jurisdictions. The international best practices in internet[78] banking will be crucial in determining the loop holes that are present in the Kenyan legal and regulatory framework.

---

[77] Ersida Teliti and Rezarta Mersini, 'Assessment of E- Banking Services and Legal Framework in Albania,' Mediterranean Journal of Social Sciences Vol 3(1), January 2012:pp267-282. <http://www.mcser.org> Assessed on 8.9.2012

[78] Mohammed Y Alem, "E- Banking and other Financial Services: Regulatory Development in selected Arab Countries": 3 <http://scribd.com/doc/66510348/E-banking-and- Other- Financial-Services-Regulatory-Developments-in-Selected-Arab- Countries.> Accessed:10/6/2012.

Mohammed Y Alem, discusses regulatory development on e- Banking and other financial Services in selected Arab countries. The author argues that the number of users of e-banking will largely depend on existing domestic and international legal support provided by the laws and regulations. Banking customers will feel more comfortable using new electronic services, if they are aware of a defined legal framework that would allow them to identify their rights and obligations with the least possible uncertainties. The necessity of updating and modernization of domestic and international legal structures has been recognized as being of utmost importance in the growth of e-banking technology. The article puts more emphasis on the role of the legal framework in adoption of internet banking. The central question for legal practitioners and lawmakers revolves around how to accommodate the use of new technology in banking and financial services in the already existing law and how to regulate it from a concrete and clear legal perspective. Accordingly, any legal and regulatory framework to govern internet banking should at the minimum revolve around the setting, enactment and enforcement of a set of laws comprising: Law on Electronic and Digital Signature; Law or Regulation on third-party Certification Authorities; Laws or Regulations on e-Banking per se; Law on Data Privacy and Laws on Anti-Money Laundering.

Johan Den Hertog[79], reviews the various economic theories of regulations.There are two broad traditions with respect to the economic theories of regulation. public interest theories of regulation and private interest theories of regulation. The first tradition

[79] "Review of Economic Theories of Regulations", Tjalling C Koopmans Research Institute, Discussion Paper Series 10-18.Utrecht School of Economics, Utrecht University,December 2010, 5<http://www.koopmansinstitute.uu.nl Assessed on 3.12.12

assumes that regulators have sufficient information and enforcement powers to effectively promote the public interest. This tradition also assumes that regulators are benevolent and aim to pursue the public interest. According to these theories, the regulation of firms or other economic actors contributes to the promotion of the public interest. Prudential banking regulations fall under Public interest theory.

Another tradition in the economic studies of regulation proceeds from different assumptions. Regulators do not have sufficient information with respect to cost, demand, quality and other dimensions of firm behavior. They can therefore only imperfectly, if at all, promote the public interest when controlling firms or societal activities. It is generally assumed that all economic agents pursue their own interest, which may or may not include elements of the public interest. The differences in objectives of economic agents and the costs involved in the interaction between them may effectively make it possible for some of the agents to pursue their own interests, perhaps at the cost of the public interest. Economic theories that proceed from these latter assumptions are therefore often called *'private interest theories of regulation'*.[80]

The capture theory assumes that in the course of time, regulation will come to serve the interests of the industry involved. According to these theories, capture is the result of the increasing power of the agency which arises because the agency in its ongoing relationship gets to know the firm better and better. The agency has thus more and more opportunities to pursue its own objective and the political principal can only control this by having more stringent administrative rules and fair and open procedures. The above theories lay down the theoretical framework that underlies this study.

---

[80] ibid

Internet banking is a relatively new technology and it is understandable that not much has been written about the topic in Kenya especially on the adequacy of the legal framework in dealing with the legal issues that arise in internet banking. It is however important to look into the aforementioned works as they give an insight to the tenets of internet banking in general and the legal and supervisory issues that arise. None of the aforementioned authors have conclusively dealt with the place of the legal framework in Internet banking. This is the gap which this research paper will try to fill by analyzing the current legal framework in internet banking and contrast it with the international best practices in the sector. The paper will identify the gaps in the framework and make recommendations on the legislative and regulatory reforms that can be made to bring it at par with the best practices in other jurisdictions.

1.9 Research Methodology

This thesis adopts an analytical approach to the analysis of legal and regulatory framework. The following research methods will be used to gain secondary data on the same:

a) Library research

b) Internet based research.

This is because the research area is a relatively novel one and the author relied on a number of texts, internet journal articles and commentaries on the emerging jurisprudence that is internet banking.

1.10 Limitation of the Study

Electronic banking is extremely dynamic especially with the introduction of the internet as a medium of e- banking technology. The law generally plays catch up with numerous changes occurring in the ICT world. Kenya's Banking Industry is governed generally by both The Banking Act[81] and Central Bank of Kenya Act[82] which have been very slow in reacting to the myriad of technological changes occurring in the banking sector. The provisions of these laws apply generally to all banking business and there are no provisions or guidelines that specifically target internet banking.

The paper shall be restricted to the domestic ream of internet banking and shall exclude discussion of cross border nature of internet banking, which raises issues of conflict of laws and jurisdictional issues. This study is limited to the analysis of the legal framework governing internet banking in Kenya. To this end other factors affecting the adoption of e- banking will be beyond the scope of this thesis and will act only as background information when discussing the topic under review

The study has not considered any African case studies since most countries in Africa are bogged down by similar issues of inadequate legal infrastructure just like Kenya. Most international case studies are from Europe, America and Asia. This is a major setback since there is no guarantee that the legislative initiatives in those countries will yield the same results, when replicated in Kenya..

1.11 Chapter Breakdown

The study is divided into four chapters as follows:

---

[81] Chapter 488 Laws of Kenya.
[82] Chapter 491 Laws of Kenya

1. Chapter One: "Introduction"

This chapter introduces the financial and legal issues being researched by this paper. This begins with an introduction/background and a statement of the research problem. It is then followed by the objectives and research questions of this paper. The hypothesis, justification of the study, theoretical and conceptual framework of the study then follows. The literature review comes after, giving an overview of some of the texts consulted in the conduct of this study. The research methodology proposed to be used during the course of the research is outlined. The chapter concludes with an assessment of some of the limitations of this study.

2. Chapter Two: "International Best Practices; Selected Case Studies"

This chapter contains an analysis of the international best practices on Internet banking as applied in other jurisdictions. It considers case studies from various countries such as: USA, UK, Singapore, and India. The chapter will also outline various model laws that govern internet banking.

Chapter Three: "Current legal and regulatory framework governing internet banking in Kenya

This chapter considers current legal and regulatory framework governing Internet banking in Kenya and identifies the legislative flaws in the framework. In addition to the Constitution of Kenya 2010, other Acts of Parliament that have been reviewed include: the Banking Act and Central Bank Act; the National Payments Systems Act 2011[83]; the Kenya Information and Communications Act 1998[84] and the Proceeds of Crime and Anti

[83] No 39 of 2011 Laws of Kenya
[84] Chapter 411A Laws of Kenya

Money Laundering Act 2009.[85] Various regulations issued by the CBK have also been discussed.

4. Chapter Four: "Findings and Recommendations"

This chapter contains the findings, conclusions and recommendations of the study. The paper identifies the gaps in the legal and regulatory framework and makes suggestions of the legislative reforms required to bring it at par with the international best practices in internet banking.

CHAPTER 2:

INTERNATIONAL BEST PRACTICES; SELECTED CASE STUDIES.

2.1 INTRODUCTION

Internet banking has presented regulators and supervisors worldwide with new challenges. The Internet, by its very nature, reaches across borders and is, for this reason, that it has engaged the attention of regulatory and supervisory authorities all over the world. The experience of various countries, as far as Internet banking is concerned, is outlined in this chapter.

The focus of this chapter will be on the legal strategies mainly revolving around the setting, enactment and enforcement of a set of laws comprising: law on electronic and digital signature; law or regulation on third-party certification authorities; laws or regulations on e-banking per se, law on data privacy and laws on prevention of money laundering. My paper argues that these sets of laws are key in the regulation of internet banking.

The above set of laws will be discussed thematically and model laws in each section identified. The legislative framework in the selected countries will be analysed based on this themes to identify best practices in the industry.

2.2 SELECTION OF INTERNATIONAL CASE STUDIES

The case studies comprise the following countries, United Kingdom, United States of America, Singapore and India. The above countries have been selected based on the following criteria;

1. The rate of online banking penetration. United States and the United Kingdom have a significant number of their total banking customers accessing internet

banking services. North America and Europe feature prominently among top ten internet users. They have developed economies where individuals are more likely to have bank accounts and regular internet access.

2. Countries that have been aggressive in reviewing their banking laws to set them in line with best practices and recent developments in electronic banking. Countries such as Singapore and India have been chosen based on this criterion.
3. The case studies take into account regional diversity. An attempt was made to make sure no two countries are chosen from the same continent.

2.3 MODEL LAWS

2.3.1 UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL) MODEL LAW ON ELECTRONIC COMMERCE[86]

The Model Law, adopted in 1996, is intended to facilitate the use of modern means of communication and storage of information, such as electronic data interchange (EDI), electronic mail and telecopy, with or without the use of such support as the Internet. It is based on the establishment of a functional equivalent for paper-based concepts such as "writing", "signature" and "original".

Key provisions[87]

The key principle underlying the Model Law is the concept of "electronic equivalence," found in Article Five. Although the Model Law does not deem electronic communications valid (just as with paper documents, legal validity depends upon more

[86] Information accessed at UNCITRAL website at < http://www.uncitral.org> on 4.12.12; The model laws are discussed based on contribution made by Professor Michael Geist from the University of Ottawa, Faculty of Law and Director of E – Commerce Law, Goodmans LLP. The professor outlined a guide to global e- commerce law.< http://*www.itu.int*>Accessed on 04.12.12

[87] Ibid, p 14

than a document's form), it provides that information or documents will not be denied legal effect or enforceability solely because they are in electronic format.

A series of functional equivalency rules specify what conditions must be met for an electronic communication to constitute a legally effective substitute for a conventional, paper-based communication. For example, Article Six provides that a legal requirement to provide information or a document sent "in writing" is satisfied by its electronic equivalent if it is in a form that can be subsequently accessed and used by the recipient.

Article Eight states that electronic documents will satisfy a legal requirement for "original" documents if there is a reliable assurance as to the integrity of the information and that the information is capable of being displayed to the person to whom it is to be presented. The question of whether an assurance is reliable is to be determined in the light of all the circumstances, including the purpose for which the document was created.

Article Eight provides that the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.

Article Nine creates an electronic equivalence standard for evidentiary purposes as it provides that evidentiary rules shall not deny the admissibility of an electronic communication solely on the grounds that it is in electronic form.

Article Ten addresses the issue of data retention. It provides that data retention requirements are met where the information contained with the electronic message is accessible so as to be usable for subsequent reference, the message itself is retained in the

format in which it was generated and any information indicating origin, destination, date and time of the message is retained.

Article Eleven of the Model Law focuses on online contracts. It removes any doubt that this popular form of online consent (clicking the "I agree" button on a website.) is valid by stipulating that unless the parties agree otherwise, an offer or acceptance of an offer can be expressed in electronic form.

2.3.2 UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES[88]

The Model Law was approved by the UNCITRAL Working Group on Electronic Commerce at its thirty-seventh session, held at Vienna from 18 to 29 September 2000. It took effect in 2001.

Key provisions[89]

Article One of the Model Law states that it applies where electronic signatures are used in the context of commercial activities. It does not override any rule of law intended for the protection of consumers.

Article Two of the Model Law defines electronic signature as "data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message."

Article Six of the Model Law provides that where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is

[88] Ibid,p 17
[89] ibid

used provided that the signature is as reliable as was appropriate for the purpose for which the data message was generated or communicated. The reliability is determined in the light of all the circumstances, including any relevant agreement.

The Model Law treats an electronic signature as reliable provided that it meets four criteria. First, the signature creation data are linked solely to the signatory. Second, the signature creation data was under the sole control of the signatory. Third, any alteration of the electronic signature, made after signing, is detectable. Fourth, where the purpose of the signature is to provide assurance as to the integrity of the underlying information, any alteration of that information must be detectable.

Article Eight of the Model Law provides that signatories must use reasonable care to avoid unauthorized use of their electronic signature. If they become aware that the security of their electronic signature has been compromised, they must notify any person that might be affected without delay.

Article 11 of the Model Law provides that a relying party will bear the legal consequences of its failure to take reasonable steps to verify the reliability of an electronic signature or to observe any limitations that may be placed on a certificate. A certificate is a data message that confirms a link between the signatory and the signatory creation data. It provides verification that the person who electronically signed a document is who they say they are.

A certification service provider is a person that issues certificates and may provide other services related to electronic signatures. Article Nine of the Model Law establishes several conduct requirements for certification service providers including:

i. to act in accordance with States' policies and practices;

ii. to exercise reasonable care to ensure the accuracy of any information found on its certificates;

iii. to provide reasonably accessible means whereby parties relying on a certificate can confirm certain information pertaining to the certificate; and

iv. to utilize trustworthy systems.

Although the Model Law does not create firm standards, it does provide that the following factors should be considered when determining trustworthiness:

a) Financial and human resources of the provider

b) Quality of hardware and software systems

c) Procedures for processing certificates.

d) Availability of information to signatories and relying parties

e) Regularity and extent of independent audits

f) Regulation or licensing by government authorities.

.3.3 EU DIRECTIVE ON E-SIGNATURES[90]

The purpose of this directive is to facilitate the use of electronic signatures and to ontribute to their legal recognition. It establishes a legal framework for electronic ignatures and certain certification services in order to ensure the proper functioning of ıe internal market.

Member States must ensure that electronic signatures meet certain legal and echnological standards to satisfy the legal requirements of a signature in relation to data n electronic form in the same manner as a handwritten signature satisfies those

[0] Ibid p18

requirements in relation to paper-based data; and that such signatures be admissible as evidence in legal proceedings.

Member States must ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification service provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate being accurate.

2.4 PRIVACY

2.4.1 THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANS BORDER FLOWS OF PERSONAL DATA[91]

The OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data were created in 1980, well before the Internet boom and the emergence of e-commerce. Although more than 20 years old, the principles found in the guidelines continue to serve as the basis for most privacy initiatives worldwide.

The guidelines feature eight privacy principles:

1) Collection Limitation Principle: There should be limits to the collection of personal data. Such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2) Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used. To the extent necessary for those purposes, data should be accurate, complete and kept up-to-date.

[91] Information accessed at the OECD website at <http://www.oecd.org.>on 4.12.12

3) Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified at each occasion of change of purpose.

4) Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the data quality principle except with the consent of the data subject; or by the authority of law.

5) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.

6) Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

7) Individual Participation Principle: An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her. An individual should have the right to receive that data and to challenge it if incorrect.

8) Accountability Principle: A data controller should be accountable for complying with measures that give effect to the principles stated above.

2.4.2 EU DATA PROTECTION DIRECTIVE[92]

The EU Data Protection directive was enacted in 1995 with Member States required to implement its provisions by October 1998. The directive's primary goal was to create a common European standard of privacy protection for the processing of personal data. The directive establishes a series of protections for individuals including the right to know why information is being collected and how the information will be used and disclosed. Individuals are also entitled to compensation for any damages that arise from failure to abide by the directive's requirements.

Although the directive does not have direct effect outside the EU, it does contain an "adequacy clause" that has had a significant effect on the privacy law frameworks of non-EU countries. Article 25 provides that Member States must ensure that the transfer of personal data to non-EU countries takes place only if the non-EU country provides an adequate level of privacy protection.

Article 25 of the directive provides that the adequacy of the level of protection of personal data provided by a non-EU country shall be assessed in the light of all circumstances surrounding the data transfer, with particular consideration given to the nature of the data, as well as the purpose and duration of the data processing.

2.5 CASE STUDIES

This section evaluates the selected case studies and illustrates how the international best practices have been implemented.

---

[92] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2.5.1 UNITED KINGDOM (UK)

The Financial Services Authority (FSA) is the regulator in the banking industry and the Financial Services and Markets Act 2000, is the statutory framework governing the business of banking in the UK. The FSA requires financial institutions to establish and maintain systems and controls for the management of their IT systems risks, having regard to their organisational structure, the extent to which technology requirements are addressed in their business strategy, the appropriateness of their systems acquisition, development and maintenance activities supporting IT systems and networks.[93] They are to maintain appropriate controls to address their information security risks, with particular regard to confidentiality, integrity, availability and authentication, non-repudiation and accountability.

Laws on E- Signature

The UK has passed the Electronic Communications Act 2000, to implement the Electronic Signature Directive.[94] Electronic signatures and the certification by a third party of such a signature are admissible in legal proceedings, partially implementing Art 5(2) of the Directive.[95]

However, the Act is silent on the legal effect of electronic signatures, leaving it to the courts to decide based on the evidential weight to be attributed to a given type of electronic signature and whether an electronic signature is capable of satisfying a legal requirement for a signature in a particular statutory context.

---

[93] see FSA Handbook, Available at www.fsa.gov.uk/handbook

[94] Section 8, gives the minister the power to modify, by way of statutory instrument, any legislation which might require amendment in order to facilitate the use of electronic communications or electronic storage.

[95] Section 7(1) of the Act.

The Court of Appeal, in the case of *Goodman v J Eban Ltd,* [96] recognised a signature produced by means of a rubber stamp as constituting an adequate signature. Per Lord Evershed M.R,

> "..... the essential requirement of signing is the affixing in some way, whether by writing with a pen or pencil or by otherwise impressing on the document, one's name or 'signature' so as to personally authenticate the document."[97]

In Re a Debtor,[98] the court rejected an argument that the signature on a faxed copy of a signed proxy forms, was not a signature for purposes of the Insolvency Rules 1986, because it was created by the receiving fax machines interpreting the signal it received. Laddie J observed that:

> "It is difficult to see why some forms of non- human agency for impressing a mark on the paper should be acceptable while others are not." [Emphasis added]

The same approach can be taken to a fax sent directly from a PC to which the signature had been attached first by scanning a handwritten signature and inserting the resulting file in the document. The above pragmatic approaches by the courts suggest that they are prepared to move with the times and recognise electronic signatures as the legal equivalent of hand written signatures.

Additionally the Electronic Signatures Regulations 2002 have been passed to support the implementation of the Act and impose liability on issuers of qualified certificates, subject to a defence if the issuer is proved to have acted without negligence. Where a party relies

---

[96] [1954] 1 Q.B 550, CA
[97] [1954] 1 Q.B 550, at 557.
[98] (No 2021 of 1995),[1996] 2 All E.R 345.

on the other party's electronic signature only to find that it has been misappropriated and applied to the transmission by a fraudster? If the fraudulent signature was supported by a qualified certificate then the certifier will owe the relying party a duty of care under the terms of the Electronic Signatures Regulations 2002. That duty extends to the accuracy of the details certified and to the fact that the indentified signatory held the signature creation device at the time the certificate was issued. Any TTP who has certified the signature will be liable applying the principles in *Hedley Byrne & Co v Heller& Partners*[99] if the party relying on a signature can establish both the existence of a duty of care and breach.

A party may be estopped from denying liability under a document that carries its electronic signatures. Thus for example, a principal may be estopped from asserting that a signature on a cheque is a forgery if he remains silent after discovering the forgery (thereby impliedly representing that the signature is genuine) and the other party relies on it as genuine as was held in *Green woods v Martins Bank Ltd.*[100] Similar test has been applied to the fraudulent use of secret test keys in a telex transmission between banks in *Standard banks London Ltd v Bank of Tokyo Ltd, Sudwestdeutsche Landesbank Girozentrale v Bank of Tokyo and Another.*[101] In that case, a bank's secret test keys were used in sending a fraudulent "key tested" telex to another bank. It was held that this could not have occurred without negligence on the part of the bank from which the telex emanated. That bank was estopped from denying the authenticity of the telex and was held liable under forged letters of credit which the telex had purportedly authenticated. These cases would suggest that a party, whose electronic signature has been misused,

---

[99] [1964] A.C. 465
[100] [1933] A.C 51
[101] [1995]2 Lloyd,s Rep. 169

will, if that party's negligence contributed to the misuse, will be unable to repudiate the resulting document as its own and/ or will be liable for damages in tort. Similar arguments could be applied to damage resulting from a breach of the encryption used in communications between parties, where this is a result of the negligence of one party or the TTP to whom security was entrusted.

Laws on data privacy

In UK, the Data Protection Act 1998 has been passed to implement EU Data Protection Directive, which aims to reconcile the tension between protection of personal data and the swift circulation and processing of data.

Laws on money laundering

Council Directive 91/308/EEC of 10th June 1991 on the Prevention of the Use of the Financial System for the purpose of Money Laundering. This was made pursuant to arts 47 and 95 of the Treaty of Rome. It recognized that the 'effectiveness of efforts to eliminate money laundering' is particularly dependent on close coordination and harmonization of national implementing measures.

Member states must ensure that money laundering is prohibited as defined in art1.

Members were unable to agree on a broad list of criminal activities to which the directive would apply. Criminal activity include drug trafficking in line with arts 3(1)(a) of the Vienna Convention.

The directive requires the member states to prevent anonymity in banking transaction by maintaining records and reporting suspicious transaction. The U.K introduced the Money Laundering Regulations 1993 to implement the directive and to secure the amendment of the Drug Trafficking Offences Act 1986(now consolidated into the Drug Trafficking Act

1994) on retaining proceeds the proceeds of drug trafficking), the Criminal Justice Act 1988 as Amended by the Criminal Justice Act 1993 (on retention of proceeds of criminal conduct and money laundering) and most recently, to confer powers to the Authority under the Financial Services Markets Act 2000 to make anti money laundering rules to reduce financial crimes[102]as empowered under Section 146 of the Act

Other laws

The EU's Electronic Commerce Directive applies in the UK and contains several articles that bear direct similarity to principles found in the UNCITRAL Model Law. Although it falls to Member States to implement the directive into national law, the directive does have direct effect in those States that fail to enact e-commerce legislation in a timely manner.

Article 10 of the directive speaks to contracts concluded by electronic means. It provides that Member States shall ensure that their legal system allows contracts to be concluded by electronic means. In particular, Member States are warned not to create obstacles for the use of electronic contracts.

The FSA has issued guidelines on advertising in U.K. by banks for deposits, investments and other securities. The guidelines include an Appendix on Internet banking. The FSA's supervisory policy and powers in relation to breaches in the advertising code (fraudulent inducements to make a deposit, illegal use of banking names and descriptions, etc.) are the same for Internet banking as they are for conventional banking.

---

[102] Mark Hapgood Qc, Paget Law of Banking,12 edn: Butterworths,pp83-99

2.5.2 United States of America (U.S.A)

Banking in the United States (USA) is regulated by both the federal and state governments. Unlike Japan and the United Kingdom (where regulatory authority over the banking, securities and insurance industries is combined into one single financial-service agency), the U.S. maintains separate securities, commodities, and insurance regulatory agencies separate from the bank regulatory agencies—at the federal and state level.[103]

There is a matrix of legislation and regulations within the US that specifically codifies the use of and rights associated with the internet and e-commerce in general, and electronic banking and internet banking activities in particular. Some important laws of general application to commercial activity over the internet within the US are the Uniform Commercial Code (UCC), the Uniform Electronic Transaction Act (UETA), which provides that electronic documents and contracts should not be disqualified as legal documents particularly because of their electronic form.[104]

Laws on e- signature

The United States has implemented the UNCITRAL Model Law at both the national and state level. Nevertheless, most of the activity initially occurred at the state level, with dozens of states using the Uniform Electronic Transaction Act (UETA), developed by the National Conference of Commissioners on Uniform State Law, as a model. When some state laws began to deviate from UETA, the United States Congress stepped in to create a uniform standard by enacting the Electronic Signatures in Global and National Commerce Act (E-Sign) in 2000.

---

[103]Shri S. R Mittal& others, "Report on Internet Banking", Working Group set up by Reserve Bank of India, 2000: 21-23

[104] Ibid, p21

The E-sign Act validates contracts concluded by electronic signatures and equates them to those signed with ink on paper. Under the Act electronic signatures using touch-tones (on a telephone), retinal scans and voice recognition are also acceptable ways of entering into agreements. The E-sign Act takes a technological neutral approach and does not favour the use of any particular technology to validate an electronic document.[105]

There are some important differences between the UETA and the UNCITRAL Model Law. First, UETA includes a consent provision that clarifies that the Act does not require a record or signature to be created, generated, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form. Second, it facilitates the use of electronic signatures for notarization of documents. Third, Section 10 of UETA features rules for where a change or error in an electronic record occurs in a transmission between parties to a transaction.

E-Sign Act specifically provides that if there is a modification to UETA, state statutes that incorporate that modification supersede the federal statute.

E-Sign Act require that consumers affirmatively consent before electronic records can be used to provide them with information that, under other law, must be provided or made available to them in writing. Consumers are also granted the right to withdraw their consent.

Laws on data privacy

The United States does not have comprehensive privacy legislation at the federal level. It has enacted a series of industry or data-specific privacy laws. These include:

a) The Gramm-Leach-Bliley Act, which covers financial privacy;

[105] ibid p23

b) The Health Insurance Portability and Accountability Act, which covers health privacy;

c) The Children's Online Privacy Protection Act, which provides children under the age of 13 with special privacy protections.

Right to Financial Privacy Act 2009 governs the use of a customer's private data. Banks and other financial institutions must inform a consumer of their policy regarding personal information, and must provide an "opt-out" before disclosing data to a non-affiliated third party.

In addition to the industry or data-specific privacy laws referred to above, the United States and the European Union have entered into a safe harbour agreement that is designed to ensure the free flow of personal data between the two parties. Without such an agreement, there were fears that the EU might begin to block data transfers to the United States on the grounds that it did not meet the Data Protection Directive's adequacy standard.

Laws on e- banking per se

Currently, all banks, whether they are 'Internet only' or traditional banks must apply for a charter according to existing guidelines. In addition, each state has a supervisory agency for the banks that it charters. Most financial institutions in the US face no prerequisite conditions or notification requirements for an existing banking. However, newly chartered internet banks are subject to the standard chartering procedures.[106]

Supervisory policy, licensing, legal requirements and consumer protection are generally similar for electronic banking and traditional banking activities. Internet banks are also subject to the same rules, regulations and policy statement as traditional banks. However,

[106] Ibid p22

in response to the risks posed by electronic banking, federal banking agencies have begun to issue supervisory guidelines and examination procedures for examiners who review and inspect electronic banking applications.[107]

To assist supervisors in monitoring the expansion of internet banking, state chartered and national banks have been required since June 1999 to report their websites' 'Uniform Resource Locators' (URL) in the quarterly reports of financial condition that are submitted to supervisors. In addition, examiners review the potential for reputational risk associated with web-site information or activities, the potential impact of various internet strategies on an institution's financial condition, and the need to monitor and manage outsourcing relationships.

Laws on anti-money laundering

The Bank Secrecy Act (BSA) requires financial institutions to assist government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion or other criminal activities. Section 326 of The USA Patriot Act allows financial institutions to place limits on new accounts until the account holder's identity has been verified.

2.5.3 Singapore

As Singapore's central bank, the Monetary Authority of Singapore (MAS) is an integrated supervisor overseeing all financial institutions in Singapore; banks, insurers, capital market intermediaries, financial advisors, and the stock exchange. With its mandate to

[107] Ibid

foster a sound and progressive financial services sector in Singapore, MAS ensures that Singapore's financial industry remains vibrant, dynamic and competitive by working closely with other government agencies and financial institutions to develop and promote Singapore as a regional and international financial Centre.[108]

Laws on e- banking and banking generally

MAS is governed by the Monetary Authority of Singapore Act, Chapter 186, which confers MAS powers to issue legal instruments for the regulation and supervision of financial institutions. In addition, MAS also has frameworks and guidelines in place on topics which cut across various classes of financial institutions. Examples of laws governing banking industry include, the Banking Act and Financial Advisers Act[109]

MAS has reviewed its current framework for licensing, and for prudential regulation and supervision of banks, to ensure its relevance in the light of developments in internet banking, either as an additional channel or in the form of a specialized division, or as stand-alone entities (Internet Only Banks).

The existing policy of MAS already allows all banks licensed in Singapore to use the internet to provide banking services. MAS is subjecting internet banking, including Internet Only Banks, to the same prudential standards as traditional banking. Singapore may grants licences to banking groups incorporated in Singapore to set up bank subsidiaries or within the bank (where no additional licence is required). MAS also

[108] Information available on the Monetary Authority website of Singapore at http://www.mas.gov.sg/
[109] ibid

admits branches of foreign incorporated virtual banks within the existing framework of admission of foreign banks.[110]

As certain types of risk are accentuated in Internet banking, a risk – based supervisory approach, tailored to individual banks' circumstances and strategies, is considered more appropriate by MAS than "one-size-fits-all" regulation. MAS require public disclosures of such undertakings, as part of its requirement for all banks and enhance disclosure of their risk management systems.[111]

For liquidity risk, banks, especially virtual banks, should establish robust liquidity contingency plans and appropriate Asset-Liability Management systems. As regards operational risk, banks should carefully manage outsourcing of operations, and maintain comprehensive audit trails of all such operations. As far as business risk is concerned, Internet Only Banks should maintain and continually update a detailed system of performance measurement.[112]

MAS encourages financial institutions and industry associations such as the Associations of Banks in Singapore (ABS) to play a proactive role in educating consumers on benefits and risks on new financial products and services offered by banks, including Internet banking services.

Laws on e- signature

The Electronic Transaction Act of Singapore governs e- signatures in Singapore. Section 3 of the Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes:

---

[110] Ibid.
[111] S. R Mittal& others, "Report on Internet Banking", p28
[112] Ibid

(a) to facilitate electronic communications by means of reliable electronic records;

(b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;

(d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

(e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and

(f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

The Act deal with recognition of electronic records and e- signature[113]; liability of network service providers;[114]secure electronic records and signatures and effect of digital signatures[115]; and duties and regulation of certifying authorities[116]

---

[113] Part II of the Act
[114] Part II of the Act
[115] Part V and VI of the Act

Provisions on data privacy

Licensed banks in Singapore are subject to statutory obligations of secrecy with respect to information relating to its customers and their accounts. This is dealt with by section 47 of the Banking Act.

There is a draft Personal Data Protection Bill that seeks to introduce personal data protection legislation in Singapore. Prior to this, Singapore did not have any over-arching legislation to protect personal data. The Draft Bill when passed will be known as the Personal Data Protection Act ("PDPA"). While the PDPA is intended to be a baseline law which will operate along with the existing sector specific laws, the PDPA is fairly ambitious in proposing to extend its provisions to organisations which may not be physically located in Singapore but are engaged in data collection, processing or disclosure of such data within Singapore.[117]

Laws on money laundering

Singapore has established strict and rigorous anti-money laundering and countering the financing of terrorism (AML/CFT) regime through its comprehensive and sound legal, institutional, policy and supervisory framework. As a member of the Financial Action Task Force (FATF), Singapore also contributes actively towards international AML/CFT standard-setting discussions at the FATF.[118]

---

[116] Part VIII and X of the Act

[117] <http://www.cliffordchance.com /publicationviews /publications 2012/08 /singapores_new _persona l dataprotection .html> on 4.12.12

[118] ibid.

2.5.4 INDIA

The Reserve Bank of India (RBI) was established on April 1, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934, to regulate the issue of bank notes and keeping of reserves with a view to securing monetary stability in India and generally to operate the currency and credit system of the country to its advantage.

The RBI prescribes broad parameters of banking operations within which the country's banking and financial system functions. The main objective is to maintain public confidence in the system, protect depositors' interest and provide cost-effective banking services to the public.[119]

Banking Regulation Act 1949 govern the financial sector in general. Other Acts governing banking include; Bankers' Books Evidence Act and Banking Secrecy Act among others.

RBI conducts financial Supervision under the guidance of the Board for Financial Supervision (BFS). The primary objective of BFS is to undertake consolidated supervision of the financial sector comprising commercial banks, financial institutions and non-banking finance companies.

Laws on e-signature

In India, e-banking and electronic payment systems preceded enactment of any law that governed digital e-commerce. At present, there are three major statutes or guidelines governing e-finance operations in India, notably, The Information Technology Act, 2000; The Information Technology (Certifying Authorities) Rules 2000.

---

[119] From the Reserve Bank of India website at: www.rbi.org/in

The Information Technology Act, 2000(IT Act)[120], provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce.

The IT Act enables:

a) Legal recognition to electronic transaction/ record;
b) Facilitate electronic communications by means of reliable electronic record;
c) Acceptance of contract expressed by electronic means;
d) Facilitates electronic commerce and electronic data interchange;
e) Retention of documents in electronic form;
f) Legal validity to digital signatures;
g) Uniformity of rules, regulations and standards regarding the authenticity and integrity of electronic records;
h) Interception of any message transmitted in the electronic or encrypted form; and
i) Prevent computer crime, forged electronic records, international alteration of electronic records fraud, forgery or falsification in electronic commerce and electronic transactions

The IT Act 2000 and the IT Rules for Certifying Authorities lay down the framework for appointment of digital certifying authorities and acceptance of digital signatures.

The passage of the IT Act 2000 is an indication of the Government's inclination towards inclination towards promoting e- commerce and e- governance while ensuring accountability.

[120] IT Act 2000 was enacted on 7th June 2000 and was notified in the official gazette on 17th October 2000.

Provisions on data privacy

Section 72, of the Information Technology Act, 2000 casts an obligation of confidentiality against disclosure of any electronic record, register, correspondence and information, except for certain purposes and violation of this provision is a criminal offence.

However, there is a feeling that the Act has not given enough power to safeguard e-banking from frauds and complexities. With many sites getting hacked and content being changed, it is felt that the IT Act should have given more powers to deal with the complexities of the virtual world.

Provisions on internet-banking

Central Bank (Reserve Bank of India(RBI) Guidelines on Internet banking in India)[121] have been passed to regulate internet banking in India. The RBI guidelines defined the operational framework on internet banking with the main focus on security issues. Though the RBI has mandated that the commonly used (Public Key Infrastructure (PKI) technology standard should be followed, no compulsory timeframe has been set for the same so far. However, the guidelines detail the organisational, operational, and supervisory structures that banks will have to implement while offering internet banking. [122]

Laws on money laundering

The anti-money laundering legal regime is governed by the Prevention of Money-Laundering Act, 2002, which came into effect on 1 July 2005.

---

[121] Rupa Rege Nitsure, "E banking: Challenges and Opportunities, Economic and Political Weekly, Vol 38 No 51/52(Dec 27 2003- Jan 3 2004): 5380

[122] Ibid

Section 12 (1) prescribes the obligations on banks, financial institutions and intermediaries:

(a) to maintain records detailing the nature and value of transactions which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;

(b) to furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed and t records of the identity of all its clients.

Section 12 (2) prescribes that the records referred to in sub-section (1) as mentioned above, must be maintained for ten years after the transactions finished. It is handled by the Indian Income Tax Department.

Other laws

India has passed the Payment Settlement Systems Act, 2007 to provide for regulation of payment systems in India and to designate the Reserve Bank of India as the authority for that purpose and for matters connected thereto. The Act provides for authorization from the RBI, with additional provisions for regulation and supervision of the payment settlement systems by the RBI. The Payment and Settlement Systems regulations, 2008 have been passed to implement the Act.

2.6 Conclusion

While existing regulations and legislations applicable to traditional banking are being extended to banks' internet banking and electronic banking services, it is recognized that internet security, customer authentication and other issues such as technology outsourcing pose unique risks. Special legislations and regulations are being framed by the regulators and supervisors for proper management of the different types of risks posed by these services.

Consumer protection and data privacy are areas which assume great significance when banking transactions are carried over a medium as insecure as the internet. Many countries are looking at special consumer protection/data privacy legislation for an e-commerce environment.

The presence of 'virtual banks' or 'Internet only banks' and the licensing requirements required for such entities are also areas which are being looked into by overseas authorities. There has also been co-operation among the regulators and supervisors to meet the challenges of 'virtual' cross border e-banking, particularly in the light of the possibility of increased money laundering activities through the medium of Internet.

Internet banking is universally seen as a welcome development, and efforts are being made to put in place systems to manage and control the risks involved without restricting adoption and use of this e- banking technology.

CHAPTER 3:

CURRENT LEGAL AND REGULATORY FRAMEWORK GOVERNING INTERNET BANKING IN KENYA.

3.1 INTRODUCTION

The previous chapter analyzed the model laws and best practices on internet banking and discussed how this laws have been implemented in various countries(case studies). This chapter delves into current laws that govern internet banking in Kenya. The paper contrasts the Kenyan laws to the best practices to banking to ascertain the major legislative laws with regard to internet

There is no specific law that deals with internet banking in Kenya. The Constitution and various Acts of parliament capture different aspects of the law as discussed below.

3.2 The Constitution of Kenya 2010

The Constitution is the supreme law of the Republic of Kenya and binds all persons and all state organs at both levels of government.[123] All laws including banking laws must be consistent with the broad fundamental principles enshrined in the Constitution.

Privacy

> "Every person has a right to privacy, which includes the right not to have the privacy of their communications infringed."[124]

Security of internet transactions is of paramount concern to most customers particularly where financial information is involved. Safeguarding the privacy of customer's financial information is imperative if the public is to embrace internet banking.[125]

---

[123] Art 2(1) of the Constitution.
[124] Art 31(d) of the Constitution.
[125] Nath, Paul Schrick and Monica Parzinger, 'Bankers' Perspectives on Internet Banking,' E-service Journal,Vol1,No1(2001):p27<http://www.jstor.org/stable/10.2979/ESJ.2001.1.1.21>Accessed: 08/09/2011.

The Central Bank of Kenya (CBK) and bank managers must ensure that law, regulations and the internal banking security procedures deal with customer privacy, threat of intrusions from hackers, and issues surrounding the interrelationship of customer anonymity on the internet and banks' responsibility to monitor suspicious activities in the internet. The CBK must ensure that customer's information is not infringed and their privacy is guaranteed in accordance with the Constitution.

Consumer rights

"The consumers have the right to goods and services of reasonable quality and to the information necessary for them to gain full benefit from goods and services."[126]

Due to the inadequate legal framework governing internet banking in Kenya, the banker-customer relationship is based on contractual terms that tend to favour the bank over the customer. The relationship is governed by clausal terms and conditions that will exempt the bank from liability from any fraud, error or malfunctions in the electronic payment systems. This creates unequal bargaining power between banks and customers compromising the fundamental principle of freedom of contract, which is a basic tenet of contract law.

Where bargaining power is persistently unequal, the concept of inequality of bargaining power serves as a justification for the implications of mandatory terms into contract, or non enforcement of a contract by the courts to protect the customers and ensure that they get value for their money.

Access to information

" Every person has right to correction or deletion of untrue or misleading information that affects the person"

[126] Art 46(1) of the Constitution.

he above provision tries to introduce two principles of data protection, namely

1. Data Integrity Principle: Data collected must be adequate, relevant, not excessive, and up-to-date.
2. Access Principle: The data subject shall have access to his own personal data and can have the data corrected if it is inaccurate, incomplete, misleading or not up to data.

egislative Shortfalls

The right to privacy, access to information and consumer rights falls under the Bill of rights provision in chapter 4 of the Constitution. The rights may be enforced by instituting court proceedings claiming that their rights or freedom have been denied, violated or infringed or is threatened[127] This is a tedious process since proceedings in *Kenya' s adversarial process take time to be heard and in some Instances the rights* sought may be overtaken by events due to passage of time.

Even after getting a declaration after a successful litigation that the state guarantees your rights and prevents the same from being violated there is no guarantee or any enforcement mechanism to ensure that the state complies with the court order.

Some of the provisions of the Bill of Rights require legislation for effective implementation in line with the fifth schedule. Example Consumer protection provision in Article 46 require an Act of parliament to implement within four years. So far some of the laws passed to implement legislation have gone ahead to put limitations on the enjoyment of the right instead of passing progressive provisions that ensures broader enjoyment of the Bill of Rights.

---

rt 22

3.3 The Kenya Information and Communications Act 1998[128]

The Act was amended in the year 2009 to provide provisions that facilitates the development of electronic commerce by promoting public confidence in the integrity and reliability of electronic records and electronic transactions.[129] This responsibility falls squarely on the Communications Commission of Kenya (CCK) which is established to licence and regulate postal, information and communications sector.[130]

deals with provisions on electronic transactions.

The Act provides for:

a) Legal recognition of electronic records.[131]

b) Validity of contracts formed by electronic means.[132]

c) Recognition of parties of electronic messages (originator and addressee). This answers the question on authentication and non repudiation: did the message originate from, and will it bind, the person who purports to have sent it?

d) Section 83E provides for Licensing for electronic certification services. Certification ensures that the message is authenticated as having emanated from the person who purports to have sent it (originator) and has not been tampered with, therefore ensuring integrity of the electronic message.

e) The Act provides for legal recognition of electronic signature.[133] The Act authorises use of electronic signatures in government and its agencies.[134] This is a

[128] Chapter 411A Laws of Kenya.
[129] Part VIA of the Act
[130] Section 3(1) and 5(1).
[131] Section 83 G
[132] Section 83 J

very significant step and sends positive signals to the public and private entities such as banks that, electronic transactions are reliable and safe therefore promoting public confidence in the integrity and reliability of electronic records and electronic transactions.

f) The Act provides for penal measures for unauthorised access and abuse of a computer system. The threats to security and privacy in internet banking occur mainly due to trespass and abuse of the computer system. The existing internet banking technology can be used to the detriment of customers and the banking institutions. There is always a high possibility that customers' sensitive information, such as PIN numbers, may be gathered due to fraud, unauthorised access, or hacking. The penal provisions seek to develop a sound framework to minimize incidences of cybercrimes and incidences of forged electronic records and fraud in electronic commerce and other electronic transactions. This will ensure the integrity of electronic messages and safeguards the privacy of customer's financial information from unauthorised persons.[135].

g) Section 84 J establishes the Universal Service Fund which shall be managed and administered by the Commission to support widespread access to, support capacity building and promote innovation in information and communications technology services. The fund will be crucial in improving the physical infrastructure that underpins provision of ICT related services such as internet infrastructure and assist individuals get the expertise required to run ICT systems. This will increase adoption of internet banking services by banks and their

---

[3] Section 83P.
[4] Section 83 S.
[5] Section 83 U

customers even to the rural areas where access is limited due to lack of adequate physical and technical infrastructure.

The Kenya Information and Communications (Electronic certification and Domain name Administration) Regulations were passed in 2010 by Legal Notice 116/2010. The regulations deal with:

a) licensing of electronic certification services;
b) recognition of foreign certification service providers;
c) obligations of a subscriber;
d) liability of certification service providers;
e) winding up provisions of operations of certification service providers ; and domain name administration.

Section 7(1) provides that, a certification service provider shall: issue and renew certificates; suspend, reinstate or revoke certificates; conduct personal identification of subscribers; publish accurate information relating to certificates; provide a repository service listing all published certificates, records of revoked certificates that may be used to verify the validity of published certificates; ensure protection of private information and safekeeping of data security; and provide time-stamp services.

Legislative Shortfalls

1. Although the provisions on electronic signatures were passed in 2009 and requisite legislation made in 2010, no progress has been made to establish a public key infrastructure. No firm has been licensed to offer certifying services by the CCK despite the law empowering them to do so. Without a mechanism to verify the identity of the parties and prevent unauthorized tampering of electronic

message thorough encryption the benefits that this law promises cannot be realized and it will not give consumers the confidence to engage in electronic transactions. This hinders the adoption of internet banking by customers or offering of banking services by the banks.

2. The penal provisions prohibiting cyber crimes can only be implemented by a sophisticated and IT literate police force. The police need specialized training on how to detect, prevent and prosecute cyber criminals. Without special training , cybercrimes will continue unabated and reduce the confidence in engaging in e-transactions.

3.4 The Consumer Protection Bill 2011

The Bill seeks to provide for the protection of the consumer, prevent unfair trade practices in consumer transactions and to provide for matters connected with and incidental thereto. The is yet to be passed to law and went through 3rd reading on 2/10/2012 .

Sections 31- 33 of the Bill provide for provisions on disclosure of information on internet agreements, delivery of copy of internet agreement and cancellation of internet agreements.[136] Disclosure of information is vital so that before a consumer agrees to enter into an internet contract, he has all vital information to make the an informed decision.

The Bill has several short comings that include;

[136] Ss 31-33 of the Bill.

Legislative Shortfalls

1. Section 3 (1) of the Act narrows the applicability of the Act and states that it applies in respect of all consumer transactions if the consumer or the person engaging in the transaction with the consumer is located in Kenya when the transaction takes place. This presumes that the Act does not apply in cross border transaction that is a reality with the internet banking transactions.
2. Although the Act has some provisions on internet agreements the same are not sufficient to protect internet banking users. Although disclosure of information is impontant it does not cure the inequality in bargain of power between the parties to an internet banking provision contract. The bargaining power is skewed in favour of banks and the law should intervene to protect the consumer from this anomaly.
3. It may be hard to cancel an internet contract because its cancellation may be governed by a different law other than Kenyan law unless Kenyan law had been chosen as the law of the contact. Internet banking contracts may be subject to jurisdiction of law and conflict of law issues.

Laws on e- banking and banking in general

3.5 The Banking Act[137] and Central Bank of Kenya Act[138]

The Central Bank of Kenya Act establishes the Central Bank of Kenya (CBK), as the regulator in the banking industry with one of its objective being formulating and implementing policy for the proper functioning of a stable market-based financial system.

---

[137] Cap 488 Laws of Kenya. An Act to amend and consolidate the law regulating the business of banking in Kenya and for connected purposes.

[138] Cap 491, Laws of Kenya.

The CBK Supervision department is a specialized unit that spearheads supervision and regulations of banks in Kenya.

There are no specific laws that govern internet banking in Kenya. The banking law applies generally to all firms conducting banking business. The oversight responsibility and management of ICT products has been placed on the board of directors and senior management of the financial institutions. The board should put in place appropriate and adequate controls in order to provide customer confidence on confidentiality, integrity and timely availability of banking services. Therefore, any provisions on constitution and conduct of the board of directors is relevant to this study.

Section 9(A) of the Banking Act,[139] empowers the CBK to vet directors, chief executive officers to be ensure that they are fit and proper to manage banking institution. If a person is found not to be fit to be in the management of a banking institution, the person shall cease to hold that office. This ensures that only qualified persons with the requisite experience hold management position in banking institutions.

Section 33(4) of the Banking Act, empowers the CBK to issue guidelines to be adhered to by institutions in order to maintain a stable and efficient financial system. The latest CBK Prudential guidelines for institutions licensed under the Banking Act were issued in 2006. The guidelines are administrative in nature and the Central bank will only take action if the management of institutions subject to such actions has demonstrated a disregard for safe and sound banking practices and/or the lack of willingness or ability to correct

[139] No director shall take up his/her position prior to being cleared by the Central Bank. The Institution shall submit to the Central Bank duly complete form CBK/IF 1-2 annexed to Guideline No. CBK/ PG/01 on Licensing of New Institutions.

weaknesses or problems on their own in line with the prudential guidelines. Relevant guidelines include;

Guideline on Corporate Governance CBK/PG/02

The Central Bank prudential guidelines (2006) on corporate governance provide the minimum standards required from directors, chief executive officers and management of an institution so as to promote proper standards of conduct and sound banking practices as well as ensure that they exercise their duties and responsibilities with clarity, assurance and effectiveness.

The Board must ensure that;

i. The banking institution has adequate systems to identify measure, monitor and manage key risks facing the banking institution and adopt and follow sound policies and objectives which have been fully deliberated.

ii. The directors must provide clear objectives and policies within which senior executive officers are to operate. These should cover all aspects of operations, including strategic planning, credit administration and control, asset and liability management etc.

iii. Clear lines and limits of authority for all levels of staff should be established. The seriousness of infringing on the authorised limits should be emphasized to staff at all levels.

This access controls are important to ensure that only authorized officer's access information control systems. Without control the banking systems would be compromised and the security of customers' information cannot be guaranteed.

The guidelines also issue a code of conduct applicable to directors, chief executive officers and management of institutions licensed under the Banking Act. The Board of Directors should ensure that all officers adhere to the prescribed code of conduct. The code deal with issues such as; conflict of interest; misuse of position and information; confidentiality; fair and equitable treatment.

Risk Management Guidelines

Internet banking exacerbates traditional banking while throwing new risk management challenges to bank supervisors and regulators. Example cross border internet banking transaction may heighten credit risk since the ability to measure credit worthiness of an individual who resides outside our national borders is more difficult than one who resides in Kenya. The risk of default in paying such a loan is higher in such an instance. Another risk that is heightened is operation risk arising from an inadequate information system, technology failures, breaches in internal controls etc. this may lead to losses. An effective monitoring process is essential for adequate managing operation risks, to detect and correct deficiencies in policies, processes and procedures (internal control system.)

The Central bank has issued Risk management guidelines. Risk management is important to ensure that the management only take risks that are warranted. The risk should be understandable, measurable, controllable and within institutions capacity to readily withstand adverse results. Excessive and poorly managed risks can lead to losses and thus endanger the bank's capital or earnings compromising its ability to meet its business objectives.

Provisions on privacy

Confidentiality of relations and dealings between the institution and its customers is paramount in maintaining the institution's reputation. Thus directors, chief executive officers and management must take precaution to protect the confidentiality of customer information and transactions. Business and financial information about any customer may be used or made available to third parties only with prior written consent of the customer or in accordance with the arrangements for the proper interchange of information between institutions about credit risks, or when disclosure is required by law.

Legislative Shortfalls

1. The CBK Act and the Banking Act do not specifically regulate internet banking despite the unique challenges the regulator, the bank and customer face due to the legal issues that arise with the adoption of internet banking. Best international practices show that it is prudent to issue a guideline on internet banking. The guideline should focus on security and detail the organisational, operational, and supervisory structures that banks will have to implement while offering internet banking.
2. Oversight management of banking business is left in the hands of the board of directors with various prudential rules to guide their conduct. The guidelines are administrative in nature and do not have legislative weight as opposed to Acts of Parliament or regulations and is difficult to monitor their compliance.
3. There are no data privacy laws in Kenya and the area remains unregulated. The Constitution under article 35 has allowed right to access personal data for purposes of ensuring data collected is accurate, complete , up to date and not misleading.

However this is not sufficient and data privacy law should be passed to govern handling of personal data.

3.6 The National Payment Systems Act 2011[140]

Before 2nd December 2011, there was no law that explicitly and exclusively dealt with payment systems. In the vacuum the Central Bank of Kenya (CBK) Act as amended in 1996 gave the Bank powers to oversee and regulate the payments systems.[141] The enactment of The National Payment Systems Act 2011 has given the Central Bank of Kenya an explicit legal framework for the regulation and supervision of payment systems and payment service providers.

Internet banking forms part of internet payments, thus bringing internet banking under the ambit of the Act.

The CBK is tasked with designation of a payment system under the Act[142]

Section 7 of the Act establishes the management body of a designated payment system as the body mandated to manage and regulate, in relation to its members all matters affecting payment instructions. The management body shall: provide a forum for the consideration of matters of policy and mutual interest concerning its members; act as a medium for communication by its members with the Government, the Central Bank, any financial or other exchange, other public bodies, authorities and officials, the news media, the general public and other private associations and institutions; and deal with and

---

[140] An Act of Parliament to make provision for the regulation and supervision of payment systems and payment service providers, and for connected purposes."

[141] Section 4A (d) of the Central Bank of Kenya Act provides that the Bank shall; formulate and implement such policies as best promote the establishment, regulation and supervision of efficient and effective payment, clearing and settlement systems.

[142] Section 3(1)

promote any other matter of interest to its members and foster co-operation among them.[143]

The framers of this Act seem to favour self regulation of the various designated payment systems via the management bodies with the CBK playing an oversight role.

Section 12, provides for licensing of a payment service provider.

Section 17, provides that Central Bank in the exercise of its role of formulating and implementing such policies as best promote the establishment, regulation and supervision of efficient and effective payment, clearing and settlement systems exercise all the powers and perform all the functions conferred and imposed on it by this Act, the Central Bank of Kenya Act and any other law.[144]

Guidelines on Retail transfer Guidelines 2010

The central bank of Kenya issued guidelines on Retail Transfers Guidelines. The guidelines define retail transfers and provide for the delivery of retail transfers by licensed financial institutions. It facilitates the provision of electronic payment services without compromising on the safety and efficiency of the National Payment System. The guideline for minimum standard for consumer protection and risk management to be adhered to by all providers of retail services. The guideline also deals with issues such as authorisation of payment service providers and regulating of outsourcing of operational functions.

Draft regulations for the provision of electronic retail transfer were also issued in 2011

[143] Section 8

[144] This include: Power to prohibit issuance of payment instruments; Power to be a participant and enforce any failure to settle arrangement; or act as a custodian of a settlement participant's settlement assets or act as a settlement agent; and regulate and supervise such system(s); Power of Central Bank to advise and direct any person regarding a payment system or a payment instrument on the application of the provisions of this Act; Power to conduct audits and inspections of a designated payment system or of an issuer of a designated payment instrument.

The CBK has also issued **E-Money Guidelines, 2010** to regulate e- money issuers and regulate the authorisation and conduct of business of e-money issuing, appointment of agents and protection of e- money issuers clients. This is an attempt by CBK to regulate money transfer systems including mobile money transfer like MPESA which have a high turnover running to millions of shillings.

3.6 The Proceeds of Crime and Anti-Money Laundering Act 2009[145]

Banking on the internet adds a new dimension to banking risks and can potentially be misused for money laundering.

The Proceeds of Crime and Anti-Money Laundering Act 2009 seeks to strengthen the country's anti-money laundering legal framework.[146] It criminalizes money laundering, provides for elaborate criminal and civil restraint, seizure and forfeiture procedures.[147] It requires reporting institutions to file reports on suspicious activities; verify their customers' identities and establish and maintain customer records and internal reporting procedures.[148] The Act also establishes a financial reporting centre to receive, analyze and disseminate suspicious transaction reports[149] and an asset recovery centre to undertake proceedings on asset forfeiture and manage assets recovered under the Act.[150]

---

[145] An Act of Parliament to provide for the offence of money laundering and to introduce measures for combating the offence, to provide for the identification, tracing, freezing, seizure and confiscation of the proceeds of crime, and for connected purposes.

[146] The Act was passed by Parliament and assented to by the President on 31st December 2009. It became operational in June 2010.

[147] Part VII,VIII, and IX of the Act.

[148] Part IV of the Act.

[149] Part III of the Act.

[150] Part VI and IX of the Act.

Financial institutions licensed under the Banking Act and the Central Bank Act, are required to adhere to the following reporting obligations as stipulated under Sections 44-47 of the AML Act:

1. To verify customer identity (KYC).
2. To monitor and report suspected money laundering activity.
3. To establish and maintain customer records for a minimum of seven years.
4. To establish and maintain internal controls & internal reporting procedures.
5. To report cash transactions beyond the stipulated minimum threshold of US dollars 10,000 or its equivalent in any other denomination.

Following the coming into operation of the Proceeds of Crime and Anti- Money Laundering Act 2009, CBK issued a guidance note to chief executives of financial institutions licensed under the Banking Act, to apprise them on their reporting obligations under the Act.[151] The highlights of the guidance include:

a) The requirement for all financial institutions to submit suspicious transactions to CBK in accordance with the Prudential Guideline on Proceeds of Crime and Money Laundering (Prevention), pending the establishment of a Financial Reporting Centre (the Kenyan financial intelligence unit).
b) Submission of quarterly declarations regarding the United Nations 1267 Consolidated Listing. Institutions to regularly review their customer database to ensure that none of the names match those on the United Nations 1267 Consolidated List which identifies individuals and entities that have been linked to the financing of terrorism.[152]

---

[151] CBK Bank Supervision Annual Report, 2010: p27< http:// www.centralbank.go.ke>Accessed: 10/09/2012.

[152] Kenya has signed the twelve major international protocols related to anti-money laundering, corruption, trans-national crime and combating terrorism. Among them is the United Nations Security Council

c) Watch-listing of designated individuals and entities contributing to conflict in Somalia. Institutions were directed to review all existing accounts to ensure that none of the accounts domiciled in their institutions were held by individuals or entities contributing to the conflict in Somalia.

d) Institutions were further advised to conduct enhanced due diligence when dealing with transactions emanating from high risk jurisdictions and high risk customers.

e) To observe and maintain the internal control measures and to ensure that staff undergo regular and appropriate AML training.

legislative short fall

The Proceeds of Crime and Anti-Money Laundering Act 2009 should be fully implemented and all oversight agencies such as Financial Reporting Centre, Asset Recovery Agency contemplated under the Act established to ensure that the concern that internet banking transactions may become a conduit for money laundering can be addressed effectively.

3.8 Conclusion

As discussed above, the law governing internet banking in Kenya is spread over several Acts of Parliament. The law applies generally without specific reference to electronic banking or internet banking.

An analysis of the legislative and regulatory framework governing internet banking as contrasted with the best practices in the industry has shown that there are a number of legislative shortfalls in the legal framework making it inadequate to deal with the legal issues in internet banking.

Resolution 1373 on combating terrorism and 1267 Sanction Committee that designates and issues lists of individuals or entities suspected to be linked to terrorism. The list can be accessed at the UN website: *<http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm>*.

The next chapter will recommend legislative and regulatory reforms that are necessary to bring Kenya's legal and regulatory framework in line with best practices in the other jurisdictions.

CHAPTER 4:

FINDINGS AND RECOMMENDATIONS

4.0 Summary of Findings

As the study has revealed, most countries have adopted use of the internet in their banking services. Some countries such as USA and Singapore have adopted legislations authorizing licensing of virtual banks or Internet Only Banks (IOB) to operate in their banking systems. These countries have some peculiar characteristics such as:

1. They are high income countries with higher market acceptance of Internet banking services. There customers are in a position to access uninterrupted internet access. This reflects the link between high income and good IT resources and skills;
2. These countries have passed the essential laws on: Electronic and digital signature; third-party certification authorities; and data privacy in addition to the laws and regulation that govern conventional banking. These laws are the bedrock of a proper legal framework to govern internet banking. This has given customers the confidence to engage in electronic financial transaction leading to higher customer acceptance of the internet business model;
3. The regulatory approach towards electronic finance in these countries can be summarized by the concept of technological neutrality: in enforcing applicable laws regulatory agencies shall make no distinction between the different channels for delivering financial services except in cases where the medium generate special risks that justify special regulatory treatment. The general framework of financial regulations and supervision applies to online financial services but specific rules relating to e-banking are introduced to address special risks where appropriate.

4. An analysis of the legislative and regulatory framework governing internet banking in Kenya as contrasted with the best practices in the industry has shown that there are a number of legislative shortfalls in the legal framework making it inadequate to deal with the legal issues in internet banking.

4.1 Conclusion

There is need for legislative and regulatory reforms in the sector to bring Kenya's legal and regulatory framework to be at par with the best practices in the other jurisdictions. The following recommendations will go a long way in reducing or eliminating the legislative short falls identified leading to a conducive environment for adoption of internet banking in Kenya.

4.2 Recommendations

1. The laws to implement the constitution should be passed so that customers enjoy their rights fully and the said legislation should be framed in a manner that expands the enjoyment of the Bill of Rights. Example of legislation to be passed relate to consumer protection which is crucial in internet banking.
2. Prudential guidelines should be given power equal to regulations to assist in implementing to ensure compliance. Currently the guidelines serve administrative functions.
3. The government should mobilise funds for the Universal Service Fund established under the Kenya Information and Communications Act, to support widespread access to, support capacity building and promote innovation in information and communications technology services. The fund will be crucial in improving the physical and technical infrastructure that underpins provision of ICT related services

4. The CBK should collaborate with bank directors and senior managers to make sure they adopt risk management supervisory approach, tailored to the bank's individual circumstances and strategies rather than the "one size fits all" regulatory approach. It should hold discussions with individual institutions who wish to embark on Internet banking to allow them to demonstrate how they have properly addressed the security systems before starting to provide such services.
5. The CBK should issue guidelines on electronic banking to guide banks in issues such as technology and security standards, privacy safeguards, application and system architecture, risk management standards etc
6. The provisions of the Kenya Information and Communication Act and its Regulations must be implemented and certification agencies licensed. The public key infrastructure should be set up to buttress the laws on e- signature and electronic transactions This will ensure that electronic transactions are reliable and safe therefore promoting public confidence in the integrity and reliability of Internet banking transactions. The banking laws should replicate this laws to govern internet banking.
7. A standard format / minimum consent requirement should be adopted by banks when drafting an internet service contract. A standard contract may be designed by the Kenya Bankers Association in consultation with the CBK, which should capture all essential conditions to be fulfilled by the banks, the customers and relative rights and liabilities arising there from. This will help in standardizing documentation and also develop standard practice among bankers offering Internet banking facility.

8. The Proceeds of Crime and Anti-Money Laundering Act 2009 should be fully implemented and all oversight agencies such as Financial Reporting Centre, Asset Recovery Agency contemplated under the Act established to ensure that the concern that internet banking transactions may become a conduit for money laundering can be addressed effectively.
9. The Consumer Protection Bill 2011 should be amended to include additional provisions to protect customers engaging in electronic financial transactions such as banks liability to the customers on account of unauthorized transfer through hacking or cases of denial of service. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers, whose terms and conditions are skewed in favour of banks as compared to customers.
10. A Data Protection Act needs to be passed to address issues to do with protection of personal data and swift circulation and processing of data. Personal data should not be processed without consent of data subject. Other principles to be enshrined in such a law include: notice and choice principle[153]; disclosure principle[154]; retention of data principle[155]; data integrity principle[156]; access principle[157] and security principle.[158]

---

[153] A data user shall inform the data subject that; the personal data of the subject is being processed; purpose of such data; provide a description of that data; and the right of data subject to request access.
[154] No personal data without the consent of the data subject shall be disclosed for other purposes.
[155] Personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. Once the purpose of collecting the information ceases, the personal data must be erased, unless erasure is prohibited by any law.
[156] Data collected must be adequate, relevant, not excessive, and up-to-date.
[157] The data subject shall have access to his own personal data and can have the data corrected if it is inaccurate, incomplete, misleading or not up to data.
[158] Data must be secured against unauthorised access, alteration, and destruction.

11. There is need for consumer awareness to make customers aware of risks inherent in doing business over the internet. This requirement will be met by making mandatory disclosures of risks, responsibilities and liabilities to the customers through a disclosure template to be formulated by either the CBK or individual banks.
12. The provisions dealing with cyber crimes under the Kenya Information and Communication Act (Section 83G -84G), or any other banking law provide for penalties for misuse and unauthorized access to a computer data, program or computer system. It does not deal with compensation of the victim of the crime. Further, the liability of banks in such situations is not clear. The banks providing internet banking may assess the risk and insure themselves against such risks in order to cushion the customer who might lose money, especially if no negligence is established on their part. Police should be trained on its provision to ensure they are able to detect and punish cyber criminals.
13. Banks should develop outsourcing guidelines to manage effectively, risks arising out of third party service providers such as risks of disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks' systems and misuse of the same, etc. Alternatively, the CBK may develop broad guidelines for use of the banking community.
14. The regulatory and supervisory framework for e-banking is continuing to evolve and the regulatory authorities all over the world recognize the need for cooperative approach in this area. The CBK should maintain close contact with regulating/ supervisory authorities of different countries and review its regulatory framework in keeping with current developments elsewhere in the world. This collaboration is

important also when dealing with cross border issues that may arise due to the adoption of internet banking and prevention of use of internet banking for money laundering activities.

15. The banks management must ensure that only the latest versions of the licensed software with latest patches are installed in the system, proper user groups with access privileges are created and users are assigned to appropriate groups as per their business roles, a proper system of back up of data and software is in place and is strictly adhered to, business continuity plan is in place and frequently tested and there is a robust system of keeping log of all network activity and analyzing the same.
16. Due to the rapid changes in technology and innovation in the field of e-banking, there is a need for constant review of different laws relating to banking and commerce. The Central bank should constitute a multi disciplinary standing committee to review the legal and technological requirements of e-banking on continual basis and recommend appropriate measures as and when necessary.

Bibliography

Books

Apostolos Ath. Gkoutzinis, Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce (Cambridge University Press, 2006). pp1-354.

Michael Brindle and Raymond Cox, *Law of Bank Payments*, (3 edn,) Thomson Sweet and Maxwell), pp255-321.

Articles

Andrea Schaechter, '*Issues In Electronic Banking: An Overview'*, IMF Policy Discussion, PDP/02/6, 2002, pp 1- 26. Available at http: //www.imf.org /external/pubs/ft/ pdp/2002/pdp06.pdf.

Arrow, Kenneth J. (1985), 'The Potentials and Limits of the Market in Resource Allocation', in Feiwel, G.R. (ed.), Issues in Contempory Microeconomics and Welfare, London, The Macmillan Press, 107-124.

Allen Berger, '*The Economic Effects of Technological Progress: Evidence from the Banking Industry'*(2003) 35 *Journal of Money, Credit and Banking*:141. Available at http://www.federalreserve.gov/pubs/feds/2002/200250/200250pap.pdf.

Bator, Francis M. (1958), 'The Anatomy of Market Failure', 72 Quarterly Journal of Economics, 351-379

Gaitungu, David N., '*Analysis of the challenges facing Internet banking in Kenya: A case of Commercial Bank of Africa Ltd.*' (2012). Available at http://ir-library.ku.ac.ke

George Kegoro, The Control of Money Laundering and Terrorist Funding in Kenya, Chap 3,pp3875

Ersida Teliti and Rezarta Mersini, 'Assessment of E- Banking Services and Legal Framework in Albania,' Mediterranean Journal of Social Sciences Vol 3(1), January 2012:pp267-282. <http://www.mcser.org> Assessed on 8.9.2012

Henry Thorton, '*Why Regulate,*' Lecture City University Business School, (4th November 1998) Available at http://fsa.gov.uk./library/communication/speeches/1998/sp19.shtml.

Johan Den Hertog, "Review of Economic Theories of Regulations", Tjalling CKoopmans Research Institute, Discussion Paper Series 10-18.Utrecht School of Economics, Utrecht University,December 2010, 5

Joskow,Paul L. and Noll, Roger C. (1981), 'Regulation in Theory and Practice: An Overview', in Fromm, Gary (ed.), Studies in Public Regulation, Cambridge, MA, The MIT Press, 36.

Kethi D. Kilonzo, '*An Analysis of the Legal Challenges posed by Electronic Banking*,' Kenya Law Review 1 (2007):p323-341. Available at http:// www. kenyalaw .org/ Downloads.../Kilonzo_electronic_banking.pdf.

Tamara Dinev and Paul Hart, '*Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use'*, e-Service Journal, Vol. 4, No. 3 (Summer 2006), pp. 25-60. Available at http ://www .muse.jhu .edu/journals /eservice _journal/v004/4.3dinev.html.

Rupa Rege Nitsure, '*E- banking: Challenges and opportunities,' Economic and Political* Weekly 38 No 51/52(Dec. 27, 2003 - Jan. 2, 2004): 5377-5381. Available at http: //www. jstor.org/stable/4414436.

Ravi Nath, Paul Schrick and Monica Parzinger, *'Bankers' Perspectives on Internet Banking,'* E-service Journal, Vol 1, No1 (2001): 21-36. Published by: Indiana University Press. Available at http://www.jstor.org/stable/10.2979/ESJ.2001.1.1.21.

Richard Nyangosi and J.S.Arora, '*Emergence of Information Technology in the Kenyan Banking Sector'*,(2009) 1-12. Available at http://gbmfconf2009.dufinance.ac.bd/papers /Emergence%20of%20Information%20Technology%20_Nyangosi_Arora.pdf .

Sarabdeen Jawahitha, Noor Raihan Ab Hamid and Mohamed Mazahir Mohamed Ishak, "Internet Banking: *'A Comparative Analysis of Legal and Regulatory Framework in*

Malaysia,' Arab Law Quarterly, 18, (No. ¾) (2003): 291-308 Published by: BRILL Available at http://www.jstor.org/stable/3382038.

Sarabdeen Jawahitha, Mohammed Ishak and Mohammed Mozahir, *'E –Data Privacy and the Personal Data Protection Bill of Malaysia'* Journal of Applied Sciences 7(5), 2007:732-742

Vladimir Zwass, 'Electronic Commerce: Structures and Issues', International Journal of Electronic Commerce vol1, No1 (1996) ,p2, <http://www.jstor.org/stable/27750797> Accessed 8.09.2011

Reports

Annual Reports, 2000- 2011, prepared by the Central Bank of Kenya, available at http://www.centralbank.go.ke

Bank Supervision Annual Reports, 2000- 2011, prepared by the Central Bank of Kenya. available at http://www.centralbank.go.ke

Basel committee on Banking Supervision: *Risk Management Principles for Electronic Banking (*May 2001) pp1-36. Available at http://www.bis.org.

Internet World Stats, aavailable at**:** http://www.internetworldstats.com/stats.htm

Kenya Vision 2030, Popular version,2007

Shri S. R Mittal& others, '*Report on Internet Banking'*, Working Group set up by Reserve Bank of India, June 2001: 1-131. Available at http://www.rbi. org .in/scripts /Publications ReportDetails.aspx.

Thesis

Sara Naimi Baraghani, '*Factors that Influence Adoption of Internet Banking*,' (Msc..diss, Lutea University of Technology, (2007)