AN APPRAISAL OF THE LEGAL FRAMEWORK ON CYBER FRAUD IN UGANDA.

A RESEARCH DISSERTATION SUBMITTED TO THE FACULTY OF LAW
KAMPALA INTERNATIONAL UNIVERSITY KAMPALA, UGANDA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
BACHELOR OF LAWS

By:

ONONYE TOCHUKWU GLORIA
REG. NO: LLB/42366/141/DF

NOVEMBER, 2017

DECLARATION

I Ononye Tochukwu Gloria do hereby declare that the content of this Dissertation are my original work and has never been presented in any Institution of higher Learning for a Degree or any other academic award. This research is intended to give an outline on the legal frame work on cyber fraud in Uganda. This research has been successfully done with the constant supervision of my supervisor Mr. Tuhairwe Herman .

NAME: ONONYE TOCHUKWU GLORIA

SIGNATURE: .....

REG NO: LLB/42366/141/DF

APPROVAL SHEET

This Dissertation entitled **"AN APPRAISAL OF THE LEGAL FRAMEWORK ON CYBER FRAUD IN UGANDA"** prepared and submitted by ONONYE TOCHUKWU GLORIA in partial fulfillment of the requirements for the degree of **BACHELOR OF LAWS** has been supervised and approved by my supervisor.

NAME OF SUPERVISOR: MR. TUHAIRWE HERMAN

SIGNATURE: .....

DATE: 8/12/2017

DEDICATION

I dedicate this dissertation to my family; parents [MR. and MRS Iorliam and to late MR. Ononye Victor Uchenna], Aunt [MRS. Ojukwu Maureen Ozomena], Sibilings [Ivan and Faith]. I owe you all a great tribute in my life for what I am because of you. May the almighty God continue bless you unconditionally.

ACKNOWLEDGEMENT

The success of this study resides with the Almighty GOD without whose intervention, guidance and grace I wouldn't have fulfilled this academic ambition.

I wish to express my sincere gratitude to my supervisor MR. Tuhairwe Herman who despite his busy schedule retained and guided me throughout the research period to the end of this dissertation.

I wish to sincerely thank and acknowledge my parents, aunt, uncles and siblings for the love, encouragement, and sustenance provided to me throughout this period.

I wish to thank the head of department public and comparative law MR. Abdulkareem Azeez in accordance to the time and guidance in which he offered in regards to this dissertation.

I wish to thank the entire school of law and Kampala international university for helping me attain my goals.

I wish to thank my cousin Bar. Victor Ojukwu, my friends: Brian Kyalisma, Degarr Mellyrissa, Matu Eve, Hatowa Chipo, Achoth Mary, Akinwumi john, for their constant assistance during the course of this research.

May God Almighty richly bless you all.

TABLE OF CONTENTS

LIST OF LEGAL INSTRUMENTS

THE CONSTITUTION OF UGANDA 1995 (AS AMENDED)

THE PENAL CODE ACT CAP 120

THE COMPUTER MISUSE ACT OF 2010

THE ANTI-MONEY LAUNDERING ACT, NO. 12 OF 2000.

THE ELECTRONIC AND POSTAL COMMUNICATION ACT 2010

THE COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME

THE MUTUAL LEGAL ASSISTANCE TREATY (MLAT)

THE EXTRADITION ACT CHAPTER 117

ABSTRACT

This Dissertation was intended to critically appraise the legal framework on cyber fraud in Uganda: It was guided by the specific objectives which included finding out whether Uganda's legal regime provides for cyber fraud, to explore the international legal regime in regards to cyber fraud and to suggest or make improvements to the law in regard to cyber fraud. Cyber-crime continues to cost Uganda billions of shillings as regulators discuss ways of containing what they call a complex problem. According to the released Annual Police Report 2013, cyber-crime cost Uganda about 18.1 billion Shillings. Another figure released by the Kaspersky Labs puts the figure at 25billion Uganda Shillings. As the Internet comes to underwrite more and more of our daily life, the vectors of attack for cybercriminals, hackers and state officials multiply, the total number of cyber-attacks grows year over year and the potential damage from cyber-attacks increases. As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals are going to attempt to steal that information. Cyber-crime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information is important in today's world. The study recommends that more focus should be put on individual training about cyber fraud and how to guard against it. Encourage companies, individuals and governments to rely more on open source software where possible to detect and counter new vulnerabilities faster. The study also recommends development of international agreements on spam, emails and other forms of web-based attacks.

CHAPTER ONE
GENERAL INTRODUCTION

1.0 Introduction

This Dissertation is intended to critically appraise the legal framework on cyber fraud in Uganda. It is guided by the specific objectives which includes finding out whether Uganda's legal framework provides for cyber fraud, to explore the international legal framework in regards to cyber fraud and to suggest or make improvements to the law in regard to cyber fraud.

1.1 Background of the study

According to the Black's Law Dictionary,[1] a cybercrime is defined as a crime involving the use of a computer, such as sabotaging or stealing electronically stored data. Generally, cybercrime is done using computers and the Internet. It is thus any illegal activity that uses a computer as its primary means of commission.

As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals are going to attempt to steal that information. Cyber-crime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information is important in today's world.

Cybercrimes take different forms such as cyber fraud, hacking, cyber theft, spamming, website cloning, cyber laundering, cyber bully/harassment, virus etc., but this study will focus on cyber

[1] 8th ed. Page 1168

fraud. When one looks at business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, these innovations have also brought unintended consequences such as credit card frauds, ATM frauds, phishing, and identity theft which results into offences and are called cybercrimes.[2]

Cyber fraud is a global challenge which cuts across all countries, it does not tend itself to any coloration in form of gender, religion, domination, political system or age. Therefore, each country suffers one form of cyber fraud or another and Uganda is no exception.

Cyber fraud could be defined to mean when credit and financial information is stolen online by a hacker and is used in a criminal manner, Cyber fraud could also be seen as the use of internet services or software with internet to defraud victims or to otherwise take advantage of them. In relation to cyber or Internet fraud, Internet fraud is defined as any type of fraud scheme that uses one or more components of the Internet such as chat rooms, e-mail, message boards or website to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions. Cyber-crime continues to cost Uganda billions of shillings according to the Annual Police crime and traffic report of 2013 indicated that there was a 14.9% surge in economic crimes, rising from 9,574 cases in 2011 to 11,006, mainly registered in banks, public service providers and non-governmental organizations (NGOs).

[2] *Joseph Migga Kizza, "Ethical and Social issues in the information age" second edition,(springer publishing, 2003).*

Cybercrime, which focuses on mobile money and Automated Teller Machine (ATM) fraud, was responsible for the loss of about sh1.5b. According to the report sh207m was transferred without the authority of telecommunications service providers between August and November 2012. The Police blame the spike in cybercrimes on the increase in the number of conmen commonly known as bafere, who exploit the lax laws. "In 2012, a total of 700 victims lost over sh1.2b by use of scheming devices from ATM locations in Kampala and other areas," the report launched by both the Police chief, Gen. Kale Kayihura and criminal investigations and intelligence directorate boss Grace Akullo, notes. Obtaining money by false pretense topped economic crimes with 8,250 cases reported. Kampala Central Police station registered the highest number of cases at 979, closely followed by Old Kampala at 607 and Katwe with 473.[3]

A total of 83 cases were reported in 2014 compared to 36 cases in 2013 resulting into a loss of about 27.1 billion shillings. The Police Report also emphasizes that some of the challenges they inquire is due to the fact that most complaints are not reported to the police for fear to lose clients especially in financial institutions.[4] A report from URN stated that Cyber fraud cost Uganda 18 billion in 2013 and In January 2014, and four Bulgarian nationals had their 20year prison sentence reduced to 9 years because they were first time offenders. The trio had been found guilty of ATM Fraud, after being caught with 38 Automated Teller Machine (ATM) cards of various identities.[5] The Uganda Police, which has a role to play in fighting cybercrime, is still ill equipped and lacks the capacity to investigate. There have been about four cases where the Computer Misuse Act, Electronic Media Act, Electronic Signatures Act and Electronic

[3] *The Uganda police Annual Police crime and traffic (report of 2013) "* http://www.newvision.co.ug/new_vision/news/1328127/cyber-crime-increases-14-police-report

[4] *The Uganda police Annual Police (Report of 2014)*

[5] *https://ugandaradionetwork.com/story/cyber-crime-costs-ugandans-ugx18b-annually-report*

Transactions Act have been used. Sophisticated crimes like computer and credit card fraud are becoming more frequent, and it stands to reason that identity theft will follow.[6] There is also a moderate level of financial fraud cases involving credit cards, personal checks, and counterfeiting. The rate of these types of crimes has increased in recent years. Skimming, which is a practice to capture personal identification information from ATM terminals, has increased in the region recently.[7]

Also recent media coverage has been rife with stories of large-scale data breaches, hacks and online financial crime. Information technology (IT) security firms such as Norton Symantec and Kaspersky Labs publish yearly reports that generally show the security of cyberspace to be poor and often getting worse.[8] There is also the challenge of mobile money transactions where the regulation is not defined yet. On one hand, the Uganda Communications Commission (UCC) is supposed to regulate the telecoms but considering that money transactions are involved, Bank of Uganda is supposed to step in though there is no enabling law to protect users. The best BOU could come up with was mobile money guidelines.[9] Therefore cyber-attacks are getting more complex, meaning thus data of bank customer's, government agencies' and money are at risk. Cybercrimes remains a global problem therefore the law making bodies and the implementing bodies also have to evolve in a flexible manner as the use of technology also advances.

---

[6] *The Uganda police Annual Police (Report of 2015)*

[7] *Uganda 2016 crime and safety report, "https://www.osac.gov/pages/ContentReportDetails.aspx?cid =19707"*

[8] *Kaspersky Security Bulletin 2014. "http://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014-Malware-Evolution.pdf".*

[9] *The Uganda police Annual Police crime and traffic (report of 2013) "* http://www.newvision *.co.ug/new_vision/news/1328127/cyber-crime-increases-14-police-report*

1.2 Statement of the Problem

According to the Annual Police Report 2013, 2014, 2015, 2016 cybercrime especially in the areas of cyber fraud has cost Uganda a lot of billions of shillings. As the Internet comes to support more and more of our daily life, the courses of attack for cybercriminals multiplies and the total number of cyber-attacks continues to grow therefore the potential damage from cyber-attacks would increase.

As one can see evidentially, cyber fraud is a cost to Uganda in so many ways for example the issue of fraud in banks is one of the most intractable and monumental problems to the Banking system. Uganda has an impressive array of structures, institutions and laws aimed at combating cybercrime such as: The Access to Information Act 2005, The Regulation of Interception of Communications Act 2010,The Anti-Terrorism Act 2002, The National Information Technology Authority Act, 2009, The Regulation of Interception of Communications Act, 2010, The Electronic Signatures Act, 2011, The Computer Misuse Act, 2011, The Electronic Transactions Act, 2011, The Uganda Communications Act, 2013, The Anti-Pornography Act, 2014. However, despite the creditable provisions made by the Acts, cybercrimes still thrives due to a number of problems some of which are the absence of trained personnel to prosecute the offenders, high unemployment rates, implementation of the laws, corruption etc. The problem of cybercrime has not only affected countries politically, socially and economically but has posed a big threat of the increase of terrorism, manifested by recruitment and the incitement of radicalization which proximately poses a serious threat to national and international security.

1.3 Objective of the study

1.3.1 General objective

The objective of the study is to critically appraise the legal framework on cyber fraud in Uganda.

1.3.2 Specific objectives

Specifically therefore the study aims

i. To find out whether Uganda's legal regime provides for cyber fraud.

ii. To explore the international legal regime in regards to cyber fraud.

iii. To suggest or make improvements to the law in regard to cyber fraud.

1.4 Research Questions

This study intends to answer the following questions:

i. Whether the existing cyber laws are adequate in guarding against cyber fraud in Uganda?

ii. Whether Uganda's legal framework adequately guards against cyber fraud?

iii. Whether there are adequate policies regarding cyber fraud under an international legal framework?

iv. Whether there are any strategies to ensure the reduction of cyber fraud in Uganda?

1.5 Research Hypothesis

i. To identifying the loopholes and gaps in the legal framework on cyber fraud in Uganda.

ii. To provide a background on cyber fraud in Uganda, examine the cyber laws and identify loopholes, gaps that would facilitate cyber fraud.

iii. To examine the opportunities and challenges cyber fraud regime faces.

iv. To provide policy and practice recommendations to curb cyber fraud.

1.6 Scope of the Study

1.6.1 Geographical scope

Uganda is a country with an independent jurisdiction, thus it is true that there are a plethora of laws enacted to combat cyber fraud and these laws are administered by relevant institutions.

However, this study is centered on cyber fraud in Uganda, with a keen interest on whether the existing cyber laws are adequate in guarding against cyber fraud in Uganda.

1.6.2 Scope of the legal frame work

This study is, however, confined to the enforcing bodies and parliamentary legislations which has been put into place to fight the crime emerged from cyber fraud. The choice of this scope is based on the frontline role the enforcing bodies plays in the fight against cyber fraud. This study therefore sets out to appraise the legal framework on cyber fraud in Uganda.

1.7 Significance of the study

In view of the prior statement of problem and the objectives of the study, the study has various significance, to which the outcome of this study will help raise awareness for different sectors of the public:

To the Government: The government is indisputably responsible for developing policies and frameworks that will eradicate cyber fraud and, consequently the research will bring more awareness to the Government, on further ways to fight cyber fraud.

To Anti-graft agencies: The workforce will be in a better position to strategize more, articulate issues and develop a more thorough rounded approach in fighting cyber fraud.

To Research groups: Those who would wish to carry out further research in this area or in related areas will find the research work very useful as it will provide them with the updated required information to be used to achieve their aim.

To the General public: Every person is a participant in this Project and will benefit from this study. Moreover, members of the public are the potential victims of cyber fraud. With the extermination of the menace through effective measures recommended under this study, the general public will benefit greatly.

To Foreign readers: Foreign readers will also benefit from the research work put together. They will no longer see Nigeria as one of the most corrupt nations in the world. Rather, they will appreciate the effort of the Nigerian government, through the EFCC, in restoring the lost integrity of the country. They may as well change the investment perspective about Nigeria and never to panic about the safety of their investment. Therefore the study will also have an economic impact on the nation.

1.8 Research Methodology

1.8.1 Research design

This study intends to follow a qualitative and library-oriented technique in order to collect data that is necessary in order to answer the research questions.

1.8.2 Study Population

The study population will focus on Uganda as a nation and would focus on decided cases, books, and articles written within their respective jurisdiction. The report gotten from these areas of research will be relevant and adequate for the study in other to answer the research question.

1.8.3 Data Sources

A number of sources of data will be used to facilitate the research topic which would include, The Constitution of both countries, Acts of Parliament, Subsidiary Legislation and Case Law.

The secondary source of data which will be sourced by reviewing of an already existing documented resources such as textbooks, journals, articles, decided cases, reports published online, newspaper articles, and other unpublished papers etc., this will be done in order to identify the existing information on the research topic.

1.8.4 Data Collection methods

Library research: this involves reading textbooks, decided cases, journals, reports and articles to extract relevant and essential data that is necessary for the research topic using this method would result in the collection of accurate data which its validity and reliability is of no detriment to this study, thus it is notably the most effective technique to collect data for the purpose of this research. **Internet research**: this involves browsing through different website which are relevant to the study.

1.8.5 Data Processing

All data collected shall be typed and edited using Microsoft Word for processing, the font style as Times New Romans, font size as 14 with the line and paragraph and line spacing as 1.5. All the data to be collected will be carefully processed which involves reducing the data to a form that will be suitable for anyone to be able to understand and interpret it well. All data collected will be edited which will involve the checking of errors and omissions, in order to ensure that there is complete accuracy and uniformity.

1.8.6 Data Analysis

The data collected and stored shall be analyzed critically in order to come up with the necessary findings needed in the study. Analysis will involve looking at the research findings, in order to interpret the situation at hand.

1.8.7 Limitations to the study

The problems are both methodological and theoretical. First and foremost, research is known to a number of research fellows as a costly venture, in terms of time, human resources, financial and other logistics. This study also disposed to such problems.

Secondly, the study will be conducted only in Uganda. This implies that the study had geographical limitations. The study may be conducted on a countrywide geographical scope, in the whole of East African countries (EAC). However, time and other logical issues may be unavailable to me. Nonetheless, I will use the resources available effectively and efficiently within the period scheduled to conduct the study.

Last and not the least not much research on cyber fraud has been carried out and published in Uganda, this automatically leaves the researcher with little sources of academic literature on which to base this study on. Though, there are legal frame work put into place and implementary bodies which the review may solve the issue in question.

1.9 Literature Review

Many critics have been made and written by authors and scholars on cyber fraud. These authors differ in their approach share similar views on cyber fraud. In this context, this section seeks to review only a few which are directly connected with the problem under investigation in this study. After the review, the researcher will be able to show the existing gap which this study seeks to fill.

Guillaume, L., et al. in an article titled "*Fighting Cybercrime: Technical, Juridical and Ethical*

Challenges,"[10] an article reviewed by parties with technical, legal, or law-enforcement backgrounds sheds light on those aspects, and attempt to proffer solutions to issues raised by cybercrime. Some of the issues raised include if we need more international cooperation processes? Would an „Inter(net) pol" be the solution, or is everything we need already there at a juridical level, as we are only lacking will, knowledge, and concrete collaboration between deciders and experts? Could we end up endangering liberties in the process of addressing cybercrime? The authors state that increasing the level of international cooperation and equipment of law enforcement agencies would enhance the fight against cybercrime. They posit that the Budapest Convention is likely to be the „way to go" in the struggle against transnational cybercrime. The writer observes that though this article is apt on the issues concerning the Budapest Convention and cooperation against cybercrime it does not deal with issues of international cooperation, solutions for challenges of law enforcement agencies and judicial systems in combating cybercrime.

Ssentogo R.[11] who argues that the Electronic and Postal Communications Act which was meant to address almost all electronic issues and communications in the country has fallen short of this intention. He is further of the view that cybercrimes are intermingled with electronic commerce like e- signature, digital signature, digital devices and e- contracts and that they ought to have been addressed because they are very important. He concludes that legal regime in Uganda in respect of cybercrimes is still wanting in that Electronic and Postal Communications Act did not address all the issues important to cybercrimes, hence, inadequate because it leaves a

[10] *Virus Bulletin Conference, (September publishing 2009)*

[11] *Ssentogo R. Legal Implications of Developments in Information and Communication Technology: An Appraisal of the Electronic and Postal Communications Act, 2010 (LDC Publishers 2012).*

big lacuna in the legal regime on cybercrimes.

Another writer is Heath cote, P.M.,[12] who discussed various issues on Information and Communication Technology generally. He discusses the role of Information and Communication Technology in business and commercial transactions and developments. He further, discusses the role of Information and Communication Technology in manufacturing industries, taking care of the society and educational developments. On top of that, computer crimes are discussed on the purview of the *United Kingdom Computer Misuse Act*, 1990 and the *Data Protection Act*, 1984.[13] He further advises some measures to be taken in order to protect Information and Communication Technology systems against illegal access and damages. Such measures she proposes are physical restrictions, encryptions and software usage. Even though Heathcoat advances useful techniques to ensure security to Information and Communication Technology devices; she falls short on what can be done in respect of the legal framework.

Gunarto, H.,[14] discusses ICT security on ethical perspectives and scientific efforts done to ensure that data are well protected. This protection should be done by encryptions, backu ps, fine walls, physical restrictions, a few to name. He gives more emphasis that ethical issues or values need be adhered to, in order to ensure that data and information are well protected. He also discusses how important are the agencies mandated to watch on information security and the importance of having new codes of ethics. He also discusses some legal issues on cybercrimes like jurisdiction, the criminal intent (*mens rea* and *actus reus)* and how the same

[12] *Heathcote,P.M., As Level ICT,Payne-Gallawary (Publishers,Ipswish, 2011, pg 2-28)*

[13] *Heathcote,P.M., As Level ICT,Payne-Gallawary Publishers,Ipswish,pg 2-28*

[14] *Ethical issues in cyberspace and IT society." (Ritsumeika Asia Pacific University. Retrieved June 24 2014).*

aids in the commission of crimes.

Sigh, Y.,[15] discusses various issues of cyber laws such as intellectual property rights in cyberspace, computer software and Patent information Technology Act among other things. On computer security, he discusses in detail the use of digital signatures basing on public key and encryption using numbers. He also discusses on security concerns in which case he suggests that law should be used to enhance security. He furthermore, suggests that there should be an appointed controller on the use of electronic signatures and certificates.

Ubena, J.[16] discusses at length on the pace of ICT developments in Tanzania and argues that in the wake of convergence on various ICT technologies, Tanzania is in the dire need of having comprehensive electronic communications legislation.

Viswanathan, A.,[17] has also discussed on cybercrimes or computer offences among many issues. He elaborates what are cybercrimes and continues to mention and explain them being hacking, bots and BOTNETS, key loggers, website defacement, malware-viruses, phishing, distributed denial of services, fishing, pharming, identity theft, spoofing, rootkits, mobile malwares, spams, to mention a few. He discusses also on electronic signatures, data Protection and privacy obligations, obscenity and child pornography, liabilities of intermediaries, government interceptions, monitoring and decryptions and enforcement issues on institutional framework.

---

[15] *ibid*

[16] *"Cyber Laws," 5th Edn,New Delhi: (Universal Law Publishing Co.Pvt.Ltd., 2012)*

[17] *"Why Tanzania Needs Electronic Communication Legislation? Law keeping up with Technology"(The Law Reform Journal, Vol 2, No.1, 2009, pg.21)*

Carol, J.M. has also discussed at length the issues on computer crimes and security[18], while carol analyses computer security premising his approach on physical and technological measures, the work at hand endeavors to discuss computer security on legal perspectives and challenges thereto. Mwingira [19] argues that, as computer crimes become more prevalent, there is also a dire need for police personnel and those without computer expertise to be trained in order to have an understanding of various basics in computer technologies.

Mambi, A.[20] is of the view that there is a big relationship on cybercrimes, privacy issues and data protection, child grooming and cyber –stalking. He asserts that computer technology has transformed the production of child pornography into a very sophisticated global industry and electronic communications has made it possible and easy to send and receive pornography. Children are therefore targets and vulnerable to child sex exposed through pornography, Invasion of privacy and online fraud, file sharing abuse (peer 2 peer), illegal advertisements and e-gambling. Like the other writes, he shares the views that it is difficult to prosecute, arrest crime offenders of cybercrimes. The guiding questions are which country has the right to arrest e-crime offenders and prosecute under the cyber space? Which court will have jurisdiction?

Bain Bridge, D.[21] discusses at length the development of computer technology and the implications thereto. He points out that computer crimes or cybercrimes is a big issue in United

[18] *Viswaanathan ,A.,Cyber Law,Indian and International Perspectives on Key Topics Including Data Security,E-Commerce,Cloud Computing and Cybercrimes, Lexis Nexis (Butterworth Wandwa,Nagpur,2012)*

[19] *Elimination of Cybercrimes in Tanzania: Law and Practice. Diss. (The Open University of Tanzania, 2013).*

[20] *Ibid*

[21] *Brainbridge, D. , "Introduction to Computer Law, Pearson, Education (London , 5th Edn, 2004 pg 1)*

Kingdom as per the survey done in 1999. The percentages traced were alarming as follows: - Pornography was 40%, hacking was 9%, viruses was 41% and fraud was 10% 45. Nevertheless, Brainbridge discussion concentrates in UK and EU jurisdiction and laws. This study at hand endeavors to assess and discuss the cybercrimes in Tanzania, though the UK and EU experiences are very helpful when assessing the Tanzanian context.

Lloyd, I. J.[22] discusses the development of ICT by tracing it back about five thousand years when there was an invention of the abacus. Lloyd argues that computers have not been regulated seriously because were considered that, their use was for mathematical purposes only. As time went on concerns on regulating computer started to carry legal importance when digitization started changing data into a commodity. Furthermore, Lloyd discusses relevant aspects of e-commerce, like e-contracts, e-taxation and computer crimes. Despite the fact that his analysis is United Kingdom based, it is very important and worthy of consideration in the study at hand.

Thus, the above reviewed literature shows that different authors have addressed and discussed the issues in relation to cyber fraud on various perspectives and dimensions. Nevertheless, no one has addressed the cybercrimes issues in the light of cyber fraud in Uganda, assessing the law and practice thereof. This study endeavors to assess critically on the Legal Framework on Cyber Fraud in Uganda and proposes some solutions.

---

[22] *Lloyd, I. J., Information Technology Law, (Butterworth 3rd Edn, London, 2000 pg 1)*

CHAPTER TWO

CONCEPTUAL PERCEPTIVE ON KEY TERMS

2.0 Introduction

Cyber fraud has taken advantage of the development of computer technologies to perpetrate their ill-motives and that with the usage of the internet in the banking sector; financial institutions have become constant targets of fraudsters.[23] It is for this reason that this Chapter is intended to focus on cyber fraud.

2.1 The Nature of Cyber fraud

It is true that the enormity of cyberspace is extending the boundaries of the possibility of attacks worldwide in that the cyber fraud is committed by the criminals in different jurisdiction through Cyberspace. The term cyberspace was first coined by the author William Gibson in his sci-fi novel Neuromancer (1984) as

"A metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse."[24]

Basing from the above given description it may be noted that the virtual world provided by cyberspace movement is borderless in nature that the "www" access does not require any

[23] Lloyd, I. J., *Information Technology Law,* 6th ed, (Oxford University Press, 2011, p.210)
[24] Gavazos, E. A., *Cyberspace and the Law, (*Cambridge-London, 1996, p. 1)

physical movement or cross border customs checks but rather transitional communication with different people in different countries, whereby this communication or actions are made by simple click on the mouse or keyboard and any such communication can travel from one country to another within minimum time frame.[25] Through the use of this virtual world, some people may use the cyberspace for better and lawful purpose while others use it for ill motive to commit illegal acts or to gain a certain economical advantage, this leads to the commission of crimes of which these days are technically referred as cybercrimes as explained hereunder.

Cybercrime can be explained in various words such as crimes that can be committed with the use of a computer and the Internet. Some define it as crimes committed on the internet using the computer as either a tool or a targeted victim.[26] From these definitions, cybercrime can be looked at from a narrow perspective and in a wider sense. Cybercrime in a narrow sense covers any illegal behavior directed by means of electronic operations that targets the security of a computer system and the data processed by them. In a broader sense (computer crime) covers any illegal behavior committed by means of or in relation to computer system or network, including such crimes as illegal possession and offering or distributing information by means of computer system or network.[27]

Thus Cyber fraud is any activity in which computers or networks are a tool, a target or a place of criminal activity and as hinted above it are committed through cyberspace.[28] Therefore

[25] Supra note 19.
[26] Ibid

[27] Ibid.

[28] Supra note 19

cybercrime can be simply referred as electronically committed crime through the use of Computer and internet and this being the case it is very difficult to apprehend the criminals when they are committing and it is also difficult to trace the perpetrator of the offence and their whereabouts because the offence is not a physical offence for which the perpetrator can be easily recognized and arrested.[29]

Cybercrimes can be committed by individuals inside and outside the system. External individuals may have unauthorized access to the system through, for example hacking[30], sniffing[31], spoofing and denial of service attacks expose banks to new security risks. Open electronic delivery channels have created new security issues for banks with respect to confidentiality and integrity of information, non-repudiation of transactions, authentication of users and access control.

Frauds and theft is said to be a breach to the security system of financial institutions' payment systems, which may have adverse effects on individual accounts or threaten institutions or networks.[32] The Federal Reserve Bank of Atlanta highlights the fact that industry statistics show payment fraud continually evolving, which is likely the reason it will never disappear and also institutions prefer to incur losses associated with fraud rather than paying the price of preventive measures.[33]

---

http://www.img.kerala.gov.in/docs/downloads/cyber%20crimes.pdf

[29] ibid
[30] Ibid
[31] Ibid
[32] Ibid.

[33] "Fight against payments fraud: The target is moving, but no everybody takes aim'

Fraud is not new to banks. Consumers transacting banking business in electronic form are likely to face problems that their counterparts transacting paper-based banking business face.[34] The difference is that e-crimes are committed in the digital environment. However, it is argued that theft is theft regardless of whether it is digital theft or traditional theft.[35] The M*odus operandi* has changed with the digital capabilities enhancing the speed, reach, and magnitude with which these crimes are executed.[36]

There is lesser need for thieves now days to use a gun and physical presence in a branch to rob banks. It is revolting to learn that, fraudsters use the same technologies that enable electronic payment innovations to perpetrate criminal intents, like identity theft and payments fraud.[37] They only need access to a networked computer giving rise to risks of transacting with unauthorized or incorrectly identified individuals in an electronic banking environment, the apparent consequences being financial losses to both customers and banks through fraud.[38]

There are numerous ways in which criminals have exploited the vulnerabilities in the open networked environment of e-banking and committed frauds. Even systems closed networks have occasionally been targets of criminal attacks. From this analysis, two major categories of

---

accessed at http://portalsandrais.frbatlanta.org/online-banking-fraud/

[34] Lukumay, Zakayo Ndobir. *An analysis of the legal basis for basis electronic banking in Tanzania.* Diss. (University of Dar es salaam, 2011).
[35] *Ibid.*
[36] Ibid
[37] *Ibid.*.
[38] *Ibid.*.

frauds can be made. These are card-based fraud and network-based fraud.

2.2 Types of cyber fraud

The section attempts to give a detailed discussion on ways in which fraud can be committed. Where possible, statistics to support the discussion will be given. It should however be pointed that, a discussion on types of cyber frauds can only be a discussion towards a very controversial issue, and how these issues are related to liability for losses handled.

2.2.1 Card-Based Fraud

Igor Pipan[39] points out that the vast growth of the payment card industry (PCI) in the last 50 years has placed the industry in the center of attention, not only because of its growth, but also because of the increase of fraudulent transactions.[40] Despite these efforts, it is on record that in UK alone cash machine fraud losses totaled £36.7 in 2009. The European Commission reports estimated credit card fraud in European Union is between €500 and €1000 million.

The UK Payment Association recognizes five types of card-based fraud: firstly, lost/stolen credit or debit card where the card is lost or stolen and then used by an unauthorized individual. Secondly, mail non receipt where the card or cards are being intercepted while being sent to the cardholders by post. Thirdly, counterfeit which is the type of fraud same as skimming, where the card information is copied from the magnetic stripe. Fraudsters often skim cards by using a device that is fitted to a cash machine or a PIN pad. This data is then transferred onto a fake magnetic stripe card and used in countries that have not yet rolled out chip and PIN.[41]

---

[39] Devos, Jan, and Igor Pipan. "The role of IT/IS in combating fraud in the payment card industry." (*The Journal of Internet Banking and Commerce* 14.3 (1970): 1-17).
[40] *Ibid.*
[41] *Supra note 39.*

Fourthly, card not present where the account information from the card is used to make unauthorized purchases over the telephone or the internet, and lastly, card ID theft where the account information is stolen by unauthorized individuals to make fraudulent purchases and can take many different forms.

Fraudsters can as well access the card systems and copy information that they may use to access customers' funds. In 2009, 60 percent of identities exposed were compromised by hacking attacks, which are another form of targeted attack.[42] The majority of these were the result of a successful hacking attack on a single credit card payment processor. The hackers gained access to the company's payment processing network using an SQL-injection attack. The attackers then installed malicious code designed to gather sensitive information from the network, which allowed them to easily access the network at their convenience. The attacks resulted in the theft of approximately 130 million credit card numbers. An investigation was undertaken when the company began receiving reports of fraudulent activity on credit cards which the company itself had processed. The attackers were eventually tracked down and charged by federal authorities.[43]

2.2.2 Network-Based Fraud

It was pointed out earlier in this Chapter that, existing banks with physical offices, ordinarily termed as 'brick-and-mortar banks, are establishing websites and offering internet banking to their customers in addition to their traditional delivery channels. There are also those banks

[42] Symantec Global Internet Security Threat Report: Trends for 2009 Volume XV, (Published April 2010)

[43] *Ibid*

which offer 'internet only' banking services with the data center or some other location serving as the legal address. These banks allow customers with the ability to make deposits and withdrawals via ATMs or other remote delivery channels owned by other institutions.

Customers may also make use of their debit and credit cards when paying goods and services in face to face, internet or telephone. For law-abiding citizens, the internet holds the promise of a huge, convenient, global marketplace, al at a bargain price. For criminals, the internet has created entirely – and lucrative-ways to seal from the more than 1 billion consumers in the world over the internet.[44] According to Singh, [45]steep rise in online banking fraud has undermined its success as few bank customers want to return to bank queues for secure transactions.

Internet banking fraud is fraud or theft committed using online technology to illegally remove money from, or transfer it to, a different bank account. The risk on the internet being used in effecting payments lies on its nature.[46] Loudon & Traver[47] underscores the fact that the internet was never designed to be a global marketplace with a billion users, and lacks many basic security features found in older networks such the telephone systems. It is open and vulnerable by design.[48]

---

[44] Loudon, K. C. & Traver, C.G., E-Commerce: Business, Technology and Society, (4th Edn, 2008, Person Education International, New York, p. 257).
[45] Singh, N. P., Online Frauds in Banks with Phishing, (*Journal of Internet Banking and Commerce*, August 2007, vol. 12, no.2)
[46] Kondabagil, Jayaram. *Risk management in electronic banking: Concepts and best practices*. (Vol. 454. John Wiley & Sons, 2007).

[47] Ibid
[48] *Ibid.*

The communication path is very complex and it may include passing through several public servers, lines or devices between the customers personal computers and the bank's internal networks.[49] The Reserve bank of India's Report on Internet Banking (2011) outlined some distinctive features of the Internet.

First, it removes the traditional geographical barriers as it could reach out to customers of different countries/legal jurisdictions. This has raised the question of jurisdiction of law and / or supervisory system to which such transactions should be subject.[50] Second, 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. Third, security of banking transactions, validity of electronic contract, customers' privacy, etc., which have been traditional banking concerns have assumed different dimensions given that internet is a public domain, not subject to control by any single authority or group of users. Fourth, 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. Lastly, a new form of competition has emerged both from the existing players and new players in the market who are not strictly banks as several policy decisions have also been made.[51]

As will be shown below, threats in security of electronic payment systems at the global level are alarming, despite efforts employed by banks to minimize security breaches. For example, in 1995, $10 million computer fraud against Citibank was the first successful penetration by a hacker into the system which transferred trillions of dollars a day around the world. Of

[49] *Ibid.*
[50] The Reserve bank of India's Report on Internet Banking (published in 2001)
[51] *Ibid.*

the $10 million dollars illegally transferred, $400,000 was not found.[52]

Hi-tech fraudsters have urbanized a new way of tricking online banking customers. One such most well-known and fast growing technique is phishing.[53] It is derived from fishing. Phishing (also called brand spoofing) is a term used for a short of fraud where phishers send out spoof email to a random database to fool the recipient in to divulging personal information like credit cards details, usernames and passwords, that can be used for identity theft. Phishing is one of the most well-known and fastest growing scams on the Internet today.

According to Singh,[54] the typical phishing scam involves an e-mail that appears as though it came from a reputable and known service institutions or company. The e- mail appears to be legitimate and the actual one. The message generally indicates that, due to problems in the institution (bank in this case) such a database updates, problem occurred in server, security/identity theft concerns, the recipient is required to update personal data such as passwords, bank account information, driver's license numbers, social security numbers, Personal Identification Numbers (PIN), and so forth. The e-mails include warning to the users that failure to immediately provide the updated information will result in suspension or termination of the account.[55]

Latest in phishing is an application of Trojan horse program. "Trojan horse" program insinuates

[52] Supra note 29.

[53] Sigh, N. P., "Online Frauds in Bank with Phishing" (*Journal of Internet Banking and E-Commerce*, August 2007, Vol. 12, no. 2).

[54] *Ibid*

[55] *Supra note 53*

itself into a user's computer via an email and directs the user of the system to website which is exactly similar to financial institution web site. Crooks pick up passwords and account numbers as soon as customer logon to these sites.

In 2009, the financial sector remained the sector most heavily targeted by phishing attacks, accounting for 74 percent of the brands used in phishing campaigns. Analysis of the data for phishing websites in 2009 indicates that the financial services sector also accounted for 78 percent of that total, which was slightly higher than 2008, when the volume of phishing websites for financial services was 76 percent.[56] Again, in 2009, the top two brands phished belonged to the largest U.S.-based multinational banks. In 2008, these brands ranked 17th and seventh in 2008, respectively. There was nearly a sevenfold increase in phishing URLs that targeted the top-phished brand in 2009 over the previous reporting period, while the second-ranked brand had almost a threefold increase. This indicates that phishers are narrowing their focus. Rather than targeting a wider range of smaller financial institutions, they are specifically targeting the largest banks that are more likely to have a higher number of customers banking online.

In the recent past, according to the UK payments association Apacs,[57] the huge rise in online banking fraud coincides with an upsurge in the number of phishing scams being run on the web and demonstrates the importance of educating bank customers about this type of crime. The similar concern is raised by Financial Services Authority (FSA), UK regulator. FSA recorded 8.000% increase in online banking frauds and identified phishing as major instrument. With

[56] *Ibid*
[57] Singh, N. P. "Online frauds in banks with phishing." (*The Journal of Internet Banking and Commerce* 1970)

the growth of phishing, customers are realizing that online transactions in particular e-commerce transactions are not safe.[58] Globally, about 30,000 phishing attacks are reported each month, of which over 80% are directed at financial institutions. Phishing attackers have targeted at financial entities such as Citibank, Wells Fargo, Halifax Bank, eBay, and Yahoo as reported by Secure Science Corporation (2013).[59]

In the UK alone, the number of recorded phishing incidents was 312 and 5059 between January to June, 2005 and January to June 2006 and it was among top 10 phishing site hosting countries from Jan 2005 to Jan 2007.[60] The amount of cash stolen in the first half of 2006 was £23.2m, the committee was told, and was likely to be £22.5m in the second half of the year. Singh points out US as leaders of top 10 phishing sites hosting countries and also experienced large number of phishing Attacks. At least 1.8 million consumers had been tricked into divulging personal information in phishing attacks, most within the past recent years.[61] The average loss per phishing attack was $1,244 in 2006, up from $256 in 2005.[62]

In an interesting case of ***American Export Isbrandtsen Lines Inc. and anr. Vs. Joe Lopez and another***,[63] a Miami businessman who regularly conducted business over the internet, sued Bank of America at the Miami Circuit Court for negligence and breach of contract for failing to provide protection for online banking risks that the bank was aware of. On the 6th of April 2004, his computer system was hacked into and US$90,348.65 was wired from his account at

[58] ibid
[59] *Ibid.*
[60] *Ibid.*
[61] *Ibid.*
[62] *Ibid.*
[63] Civil Appeal No. 1776 of 1971

Bank of America Direct, its online portal, by Latvian cyber criminals, to Parex Bank, a bank in Riga, Latvia without his approval. About US$20,000 of the money was withdrawn before the account was frozen by the Latvian bank. A subsequent Secret Service investigation requested by the bank detected the presence of the 'core flood *keylogging Trojan'* on his computer.

Lopez claimed that Bank of America had knowledge of the Trojan horse virus known for infiltrating and compromising security systems and enabling unauthorized access to infected computers, and therefore the bank had a responsibility to inform its customers of the virus. Further the bank should have been alerted when the transfer of such a large sum to Latvia was initiated. Latvia, along with Russia, Eastern Europe, and the other Baltic states is known for having a high level of cyber-criminal activity and thus a large monetary transfer to that part of the world should have been questioned by the bank.

To make matters worse the bank failed to act upon being notified within minutes of the unauthorized transaction and refused to assist in liaising with the Latvian bank to freeze the monies or release the balance to Lopez. It was only in July 2004, that the bank sent a letter to its users alerting them to a new "dual administration" feature requiring the approval of at least two individuals to execute a funds transfer. The letter also recommended that clients install antivirus software. Bank of America denied liability for the loss since its systems were not hacked into and all appropriate measures were taken to complete the transfer.

2.2.3 Banks' Employees Fraud

Employees of the institution are frequently the source of electronic banking crime. [64] They are likely to have access to the systems and often can mask criminal actions behind legitimate activities. They may hide unauthorized procedures within programs (the "Trojan horse" strategy) by building in instructions to abort or divert authorized transactions, and then remove this procedure from the computer's memory bank. Unauthorized copying of either programs or data, such as account numbers and personal identification numbers (PINs), usually cannot be detected or traced. It is for this reason that many incidents of e-crimes are difficult to detected when they are committed by insiders, who have a good understanding of the systems and controls and are thus able to exploit the loopholes without leaving trace.[65]

Talwar[66] recounted a reported incident of an IT expert who could penetrate the multilayer password system governing the fund transfer facility of the bank, which was allowed to be self-operated by its corporate customers. He could successfully effect wire transfer of millions of dollars from a corporate account to his own and wife's account across continent to a destination in Europe. Though the corporate treasury manager of the customer was watching the fund transfer stolen and shifted before his very eyes, he was helpless in the context of such operation happening in few seconds. While the cyber fraud was possible in seconds, the efforts of law enforcement took time to cross the continental legal and criminal enactment barriers to overcome before they could ultimately nab the above criminal.

---

[64] *Buckhoff, Thomas A. "Employee fraud: Perpetrators and their motivations." (The CPA Journal 71.11 (2001): 72).*

[65]

[66] Talwar, S. P. "Computer Crime - an Overview"

In Nigeria, 600 Euros Electronic Funds Transfer fraud perpetrated through a bank in Benin, Edo State. The amount was sent by an Irish businessman, Kevin Fuller, to his Nigerian partner through Western Union Money Transfer at 5.28pm Nigerian time on 3rd November 2008 from Dublin Ireland. The money was collected by a yet to be identified person at exactly 6.22pm Nigerian time on the same day. The inward transfer and outward payment took place after 4pm when banks had closed their doors to outside customers.

2.2.4 Money Laundering Using Electronic Banking

The offence of money laundering is now being committed using computers and computer networks, the internet inclusive. The imminent danger with the use of the internet is that transactions become instantaneous, untraceable and may easily be anonymous, leaving no audit trail.[67] As shown below, the use of computer technologies to perpetrate the offence of money laundering is currently not a new thing in Uganda.

2.3 Incidents of Cyber Frauds and Unauthorized Transfer in E-Banking in Uganda

As pointed out earlier in this study, clear manifestations of breach of security in e- banking include frauds, identity theft and unauthorized access to customers' accounts leading to unauthorized transfers of funds. A few incidents of fraud, unauthorized transactions and identity theft that occurred in Uganda show that Uganda is not an exception. The process of stealing money or property by using computer is called computer/cyber fraud which can be done in two ways. The first is by using a forged bank card, and the second is by giving instructions to the computer to transfer funds from one bank account to another.

[67] The Reserve Bank of India, "Internet Banking Report" op.cit., at p. 81

The reasons for the increase of cyber frauds in the banking sector include the presence of unfaithful staffs, lack of effective internal controls as well as willingness to share negative information among financial institutions and with law enforcers.[68] A few incidents below show that consumers transacting banking business in electronic environments face problems related to fraud leading to loss of their money.

There are a few incidents on unauthorized access to customers' accounts which were referred to courts of law. The first one involved three appellants who are Bulgarian Nationals who entered Uganda on diverse days. They were arrested at Natete Stanbic Bank Branch when the first and second appellants had fixed an ATM skimmer device which is an ATM card reader on the branch's ATM machine capture to PIN numbers from ATM Cards. They were travelling with the 3rd appellant and the fourth accused who was acquitted by the High Court on appeal. The vehicle they were travelling in was searched and 37 cloned carvel ATM cards were recovered. Also recovered from the car was a list of numbers which were later found to be Personal Identification Numbers (PIN) of customers of Stanbic Bank. Other items were recovered from the car and others from their residence in Nalya.

The 3 appellant's were convicted in respect of 33 cards on the 33 counts of forgery. They were also charged and convicted for committing a felony c/s 390, 342 and 347 of the Penal Code Act and were also convicted for unauthorized access to Computer Data without authority c/s 12(1) of the Computer Misuse Act in count 36. They appealed against the conviction and sentence and the High Court altered the sentences still they were dissatisfied with the High Court decision

[68] The Speech by the Governor of the United Republic of Uganda during an opening occasion of the Uganda Bankers Association Workshop on Collaborative Approach in Combating Financial Crimes in the Banking Industry (on 22nd July, 2010 in Kampala).

hence this second appeal.[69]

At the hearing of the appeal the appellants were represented by learned counsel, Mr. Ochen Evans. The State was represented by Mr. Emmanuel Muwonge a Principal State Attorney. The decision of Court:

The appeal in the instant case is against sentence and not against conviction. The appellants are praying to this Court to set aside and or vary the sentences. Thus In respect of ground one therefore we would retain the 2 years sentence for counts 23, 29 and 30 to run consecutively. The appellants would in total serve a total sentence of six years imprisonment. We so order. And also quashed the deportation order by the High Court Judge. We substitute it with the order of the Magistrate Grade One against which no appeal was preferred.

The second incident involved four accused persons. In this case, Guster Nsubuga (A.1), Mugere Farouk Ngobi (A.2), Owora Patrick (A.3) and Byamukama Robinhood (A.4) are jointly indicted. Four of the charges are derived from the Computer Misuse Act while the other two are drawn from the East African Community Customs Management Act. The charge in count I is unauthorized use and interception of computer services, contrary to sections 15(1) and 20 of the Computer Misuse Act said to have resulted in a loss of shs 2,461,447,275 and 78 cents. In count II the charge is Electronic Fraud, contrary to section 19 of the Computer Misuse Act which is said to have resulted in the loss of shs.2, 461,447,275 and 78 cents. The charge in count III is unauthorized access to data, contrary to sections 12(2) and 20 of the Computer Misuse Act. In count IV the offence is producing,

[69] Gachev & Ors v Uganda (CRIMINAL APPEAL NO. 155 OF 2013) [2016]

selling or procuring, designing and being in possession of devices, computers, computer programmes designed to overcome security measures for protection of data, contrary to sections 12(3) and 20 of the Computer Misuse Act. The charge in count V is unauthorized access to a customs computerized system, contrary to section 191(1) (a) of the East African Community Customs Management Act 2009 resulting in the loss of tax revenue of shs 2,461,447,275 and 78 cents. The offence charged in count VI is fraudulent evasion of payment of duty, contrary to section 203(e) of the East African Community Customs Management Act 2009.

Nsubuga Guster, the first convict, and Robin hood Byamukama, the other convict, singularly and through their counsel express their regret for what they did and ask this court to be lenient when passing sentence. Besides their young age both told court that they have families and that they are bread winners for their respective families. The state on the other hand seeks for a stiff sentence to be handed down to each of the convicts arguing that what they did resulted in tremendous loss to the exchequer of URA and compromised the security system of the country. Doubtless it shakes the faith people here and abroad have in that body fondly known as URA. Ramifications of Cybercrime are not as obvious as those of robbery for instance in the short term. In the long run one notices the greed of those who seek to disinherit the poorest of the poor through discreet methods such as the convicts sought to employ and did apply to sordid effect. The judge in his sentence stated that "I have anxiously considered the recommendation of the prosecution to invoke S.20 of the Computer Misuse Act where convicts in like offences are liable to life imprisonment for offences under count 1, count 3 and count 4. I note the convicts have no previous record and that they are relatively young men. I have taken into account the period they have spent on

remand and the fact that they have young families. Of course I bear in mind their remorse. Consequently I sentence each of the convicts to 12 years' imprisonment on count 2. On count 1, 3, and 4 I sentence each one of them to 8 years' imprisonment. On count 5 each of the convicts is sentenced to a fine US$4,500. The custodial sentences are to run concurrently".[70]

The third incident was on 25th January 2013 in the case of ***Uganda v Sserunkuma & 8 Ors*** [71]where a sum of shs 3,150,000,000/= was transferred from the MTN Dispute Account in seven equal installments of shs 450,000,000/= each to MTN Agent lines employing fraudulent means. A detailed explanation was given regarding how the mobile money system operates, by PW2 in particular. It was stated that the system operates in an external environment which involves banking and agents as well as subscribers on one hand. On the other hand there is the internal system called fundamo specifically for mobile money .Within fundamo there is the bank control account and the dispute account. A deposit is made by an agent on an escrol account in the Stanbic Bank. That deposit is then electronically synchronized into fundamo through the dispute account and onward to the intended beneficiary. This should happen without manual intervention. The loss was to MTN consequently .It was prosecution case that the money which went into agent lines was later transferred to a total 138 subscriber accounts and that it was withdrawn in cash or tokens. Immediately this was detected the system was closed and investigations commenced. None of the accused persons was arrested in the course of committing the offences alleged against them. The prosecution arrested them subsequent to the transactions and assembled what evidence there was linking them to the charges. That evidence

[70] Uganda v Nsubuga & 3 Ors (HCT-00-AC-SC-0084-2012) [2013]
[71] (SESSION CASE NO. HCT-00-CR.SC 15/2013) [2015] UGHCACD 3 (27 April 2015)

was largely circumstantial. To justify an inference of guilt the inculpatory facts must be incompatible with the innocence of the accused and incapable of explanation upon any other reasonable hypothesis than that of guilt.

The jugde in his sentence Regarding electronic fraud in count 6, stated I have considered that the offence was premeditated, that it is on the increase, that the community stands to lose confidence in the mobile money systems and that the complainant is sapped of credibility by such activities. I have considered that were this to continue it would impede social progress. I have also considered the youthful ages of the perpetrators and their domestic responsibilities. I have taken into account the period of over 2 years spent on remand. I deduct that period from the possible sentence I would have given. I sentence A1, A2, A3, A4 and A5 each to 7 years' imprisonment.

As pointed earlier in this chapter, mobile banking is an innovation in Uganda. Despite being a new distribution channel in Uganda, fraudsters are increasingly using it to steal money from customers' accounts.

The main reasons are negligence of customers in not keeping safe their cards and Codes and ignorance in using the ATMs to either withdraw or transfer money. A customer, for example, who has little or no knowledge in using an ATM may request another customer to assist. In the course of assisting him or her, he/she records the PIN as well as the number of the account and later uses these records to register in NMB Mobile as a genuine customer. He/she then transfers money from the customer's account to his own or some other person's account, after which he could now either transfer the money or withdraw using an ATM card.

The customer may at a later stage discover that there is an amount of money or all the money

in his/her account missing. In case he/she reports to the bank about the loss, the bank would at best assist him to trace the mobile phone number used to transfer the money. The customer would be lucky if the thief did not throw away or destroy the line he/she used. At times it proves very difficult to trace the person. In case efforts to trace the thief become successful, investigations leading to the thief being charged in Court would be made.

Computers and computer networks including the internet are now used to commit the offence of money laundering.[72] The imminent danger with the use of the internet is that transactions become instantaneous, untraceable and may easily be anonymous, leaving no audit trail. The use of computer technologies to perpetrate the offence of money laundering is currently not a new thing in Uganda. Several incidents that have been reported over the media and some which have landed to courts of law is evidence to this fact.

The relevance of bringing these incidents to light which led to massive losses of both banks' and customers' money is three fold. First, in order for electronic funds transfer involving huge amounts of money to be successful, there must in most cases be an involvement of an employee of the bank. Second, the customers' monies in banks are not safe due to the presence of unfaithful employees, who have access to customers' accounts information. Third, bank customers may conspire with employees of the banks in order to allow crime to be perpetrated using their accounts.

2.4 Conclusion

The aim of this chapter was to show the nature of cyber fraud, its types, how and ways

[72] The Reserve Bank of India, "Internet Banking Report" op.cit., at p. 81.

in which it runs, in and out of Uganda. It defined e-crime and identified a few incidents of cyber fraud at the international level, the purpose being to lay a foundation for recommendations of a suitable legal framework in Uganda.

CHAPTER THREE
LEGAL FRAMEWORK ON CYBER FRAUD IN UGANNDA

3.0 Introduction

The purpose of this Chapter is to present a discussion on how the penal laws address the cyber fraud in Uganda. It will show that the existing legal framework on criminal law has no such offences referred to as cyber fraud. It is doubtful whether the existing principles on criminal law designed to regulate paper –based transactions can apply to theft and frauds in electronic banking. However, this point is being increasingly recognized as an area of concern and more and more countries are, therefore, enacting specific and comprehensive legislation to cover the acts of computer criminals.

3.1. Cyber Fraud Legislation in Some Africa countries

The East Africa region includes Uganda, Kenya and Uganda, while the Southern African Development Community (SADC) region includes Zambia, Zimbabwe, South Africa, Malawiand Mozambique. The SADC region started harmonizing cybercrime laws in 2006 to deal with cross-border criminals. The new laws allow member countries to prosecute cybercriminals despite where the crime was committed in the SADC region.

However, progress has been slow in several countries, such as: Kenya and Uganda who have not proposed draft laws to their respective parliaments. Mauritius, South Africa and Zambia have adopted cybercrime legislation. Botswana finally has a cybercrime law, passed by Parliament in December 2007 and signed into law by President Festus Mogae later in the same month.

3.2 Legal Framework on Cyber fraud in Uganda

3.2.1 THE PENAL CODE ACT CAP 120

The Penal Code Act (PCA) prescribes liability and punishments for crime.

As pointed out above, persons who used mobile phones and ATM cards to transfer money from other persons' accounts in Uganda have been charged with the offence of theft contrary to **section 254 of the Penal Code, Cap. 120** Which provides that:

254. Definition of theft.

(1) A person who fraudulently and without claim of right takes anything capable of being stolen, or fraudulently converts to the use of any person other than the general or special owner thereof anything capable of being stolen, is said to steal that thing.

It appears that the above section does not create the offence of cybercrime; it rather provides punishment for the offence of theft. **Section 254** defines the offence of theft while **section 253** stipulates things that are capable of being stolen. The elements of the offence of theft according to **section 254** consist of anything capable of being stolen, act of appropriation, a certain type of property, unlawfulness and intention, including an intention to appropriate.

From the elements of the offence of theft only tangible things that are capable of being moved from one place to another may be stolen. That being the case, it is questionable whether or not theft may be committed in e-banking transactions. As stated earlier in Chapter Two of this study, computers are currently used to process, store and disseminate data involving monetary value. When a person accesses a computer or an intelligent device, he has a number of motives, one being to transfer money. At that time he is moving data with monetary value and later he accesses money using an ATM machine. It is doubtful whether information or data could qualify

as a subject of theft. This is a *lacuna* in the legal system in Uganda. It is argued in this study that the law must define the term 'property' or 'thing' to include incorporeal property or thing in order to render data or information capable of being stolen.

The closest offences in relation to computer data theft are unauthorized access to the computer and unauthorized access with ulterior intent.

As also observed above, suspects of e-crimes in Uganda are also charged with the offence of forgery contrary to sections 342, 344 and 345 of the Penal Code, Cap 120.

342. Forgery.

Forgery is the making of a false document with intent to defraud or to deceive.

344. Bank note and currency note.

In this division of this Code, "bank note" and "currency note" include any notes, by whatever name called, which are legal tender in the country in which they are issued.

346. Intent to defraud.

An intent to defraud is presumed to exist if it appears that at the time when the false document was made there was in existence a specific person, ascertained or unascertained, capable of being defrauded by it, and this presumption is not rebutted by proof that the offender took or intended to

take measures to prevent such person from being defrauded in fact, nor by the fact that he or she had, or thought he or she had, a right to the thing to be obtained by the false document.

Forgery in banks can take a number of forms. First, a person forges a transfer statement that

authorizes movement of funds from one account to another. The form in this respect is paper-based, but the actual transfer is done electronically, different to when a cheque is involved. Once the form is accepted by the bank the transfer becomes instantaneous and it cannot be reversed.

The second type of forgery is when a person counterfeits someone's plastic card and uses it to withdraw funds from the account belonging to that person. For access to the account to be possible, the thief or fraudster must have knowledge of the person's PIN or Code. For example in the case of **Odama & Anor v Uganda (NO. HCT-00-CN 0017/2015) [2015] UGHCACD 15 (6 October 2015);**

Lukuba Benson and No.37175 PC Odama Edward between 14th and the 20th February 2013 conspired to personate an officer of the Inspectorate of Government in order to obtain money from Kisira Baptist, the Speaker of Kaliro Town Council to allegedly halt investigations into the alleged sale of Kaliro Town Council building to Tropical Bank.'

The third is when a person sends electronic instructions to authorize transfer of funds whereas he has no such authority to do so. For example, a person may send an email to the bank instructing it to transfer funds from one account to another. As was seen in the case of **Uganda v Nsubuga & 3 Ors** [73]

Section 342 of the Penal Code cap 120 defines the offence of forgery as the "making of a false document with intent to defraud or to deceive." From the provision of section 345 of this law, a person would be guilty of the offence of forgery if he

[73] Supra note 72

345. Making a false document.

Any person makes a false document who—

(a) Makes a document purporting to be what in fact it is not;

(b) Alters a document without authority in such a manner that if the alteration had been authorized it would have altered the effect of the document;

(c) Introduces into a document without authority while it is being drawn up matter which if it had been authorized would have altered the effect of the document

(d) Signs a document—

(i) In the name of any person without his or her authority whether such name is or is not the same as that of the person signing;

(ii) In the name of any fictitious person alleged to exist, whether the fictitious person is or is not alleged to be of the same name as the person signing;

(iii) In the name represented as being the name of a different person from that of the person signing it and intended to be mistaken for the name of that person;

(iv) in the name of a person personated by the person signing the document, if the effect of the instrument depends upon the identity between the person signing the document and the person whom he or she professes to be.

From the provisions of the law in relation to forgery as pointed out above, it is arguable whether criminals who transferred funds using electronic messages that have been forged or cards that have been counterfeited can be brought to justice. In the circumstances, where the fraud involves electronic transfer of data the computer misuse Act shall apply, whereas where the transfer of data does not involve any electronic transfer of information Cap 120 shall prevail as

appraise above.

3.2.2 THE COMPUTER MISUSE ACT OF 2010

The Computer Misuse Act (CMA) prescribes liability for offences related to computers.

Section 18 unauthorized disclosure of information.

Which states that Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access.

A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

Section 19[74] **provides for Electronic fraud;**

A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both. For the purposes of this section "electronic fraud" means deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.

[74] Supra note 72

Section 20[75] **provides for enhanced punishment for offences involving protected computers**; where access to any protected computer is obtained in the course of the commission of an offence under **section 12, 14, 15**[76] or the person convicted of an offence is, instead of the punishment prescribed in those sections, liable on conviction, to imprisonment for life. Or the purposes of **subsection (1)**, a computer is treated as a "protected computer" if the person committing the offence knows or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for—

i. the security, defence or international relations of Uganda

ii. the existence or identity of a confidential source of information relating to the enforcement of a criminal law

iii. the provision of services directly related to communications infrastructure, banking and financial services, public utilities or public key infrastructure

iv. The protection of public safety including systems related to essential emergency services such as police, civil defense and medical services.

For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in **subsection (2)**.

Section 21[77] **provides for Abetment and attempts;**

a person who abets another person in committing an offence under this Act, commits that offence and is liable on conviction to the punishment prescribed for the offence.

[75] Supra note 72
[76] Ibid
[77] Ibid

Any person who attempts to commit any offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence.

Section 22[78] defined Attempt

as when a person, intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfillment, and manifests his or her intention by some overt act, but does not fulfill his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence.

It is immaterial except so far as regards punishment, whether the offender does all that is necessary on his or her part for completing the commission of the offence, or whether the complete fulfillment of his or her intention is prevented by circumstances independent of his or her will, or whether the offender desists of his or her own motion from the further prosecution of his or her intention or that by reason of circumstances not known to the offender it is impossible in fact to commit the offence.

Section 27[79] provides for Compensation;

Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act.

[78] Supra note 72
[79] Ibid

3.2.3 Anti-Money Laundering Act, No. 12 of 2000.

Sections 12(b) creates the offence of money laundering in the following words

12. A person who –

(b) Converts, transfers, transports or transmits property while he knows or ought to know or ought to have known that such property is the proceeds of a predicate offence, for the purpose of concealing, disguising the illicit origin of the property or of assisting any person who is involved in the commission of such offence to evade the legal consequences of his actions.

A list of predicate offences is given under **section 3** of the Act, some of which are illicit drugs trafficking, terrorism, illicit arms trafficking, corrupt practices, counterfeiting, armed robbery, theft, forgery, tax evasion, illegal mining and environmental crimes. A person who is guilty of the offence of money laundering shall be sentenced to a fine not exceeding five hundred million shillings and not less than one hundred million shillings or to a term of imprisonment not exceeding ten years and not less than five years. [80] The money laundering Act does not mention anything to do with electronic transfer or fraud however, given its nature it is a common practice that money launderers often use electronic transfer of fund to disguise the source of their money. Therefore the money laundering Act is critical to the researcher study for purposes of a proper appraisal of the topic.

There is no mention of electronic crimes in the list and one wonders why the omission despite

[80] Section 12 of the Anti-Money Laundering Act of 2006.

the Act being enacted in 2006 when ICT had already gained a very important place in the operations of banking business.

As seen above, the culprits transfer money electronically from one account to another with ease, instantaneously and without the ability to trace it. It is doubtful whether the interpretation of the term "transfer" includes an electronic transfer. This doubt is justified by the fact that the Act makes no mention of electronic transfer.

Indeed, it does not even define the term 'transfer'.

3.2.4 Electronic and Postal communication act 2010

Section 116 provides :

i. Any person who installs, operates, constructs, maintains, owns or makes available network facilities without obtaining any relevant individual license, commits an offence and shall be liable upon conviction to a fine of not less than five million Ugandan shillings or imprisonment for a term not less than twelve months or to both.

ii. Any person who provides network services without obtaining any relevant individual license, commits an offence and shall be liable upon conviction to a fine of not less than six million Ugandan shillings or imprisonment for a term not less than twelve months or to both.

iii. Any person who –

(a) Provides application services without having first obtained any relevant individual license;

(b) Provides content services without having first obtained any relevant individual license, or any relevant class license commits an offence and shall be liable upon

conviction to a fine of not less than five million Ugandan shillings or imprisonment for a term not less than twelve months or to both;

(c) Imports, distributes, or sells electronic communication equipment or apparatus or; establishes, installs, maintains and operates an electronic communication system or imports non type approved electronic communication equipment or apparatus into the United Republic without a license, commits an offence and shall be liable upon conviction to a fine of not less than five million Ugandan shillings or imprisonment for a term not less than twelve months or to both.

Section 118[81] makes an offence to create obscene communication like child pornography and other offence of such nature. Section 118 of the same Act run as hereunder,

Any person who-

i. By means of any network facilities, network services, applications services or content services, knowingly makes, creates, or solicits or initiates the transmission of any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person;

ii. Initiates a communication using any applications services, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to

Annoy, abuse, threatens or harass any person at any number or electronic address;

[81] Ant-money Laundering Act

By means of any network services or applications service provides any obscene communication to any person; or

iii. Permits any network services or application services under the person's control to be used for an activity described in **section 117 (3)**[82],commits an offence and shall, on conviction, be liable to a fine not less than five million Ugandan shillings or to imprisonment for a term not less than twelve months, or to both and shall also be liable to fine of seven hundred and fifty thousand Ugandan shillings for every day during which the offence is continued after conviction.

iv. **Section 120**[83] creates a penalty for interception of communication and it provides that: Any person who, without lawful authority under this Act or any other written law- Penalty for interception of communications

(a) Intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept any communications; or

(b) Discloses, or attempts to disclose to any other person the contents of any communications, knowingly or having reason to believe that the information was obtained through the interception of any communications in contravention of this section; or

(c) uses, or attempts to use the contents of any communications, knowingly having reason to believe that the information was obtained through the interception of any communications in contravention of this section, commits an offence and shall, on conviction, be liable to a fine of not less than five million Ugandan shillings or to imprisonment for a term not less than twelve months, or to both.

[82] Supra note 81
[83] Ibid

Under that **Section 120**[84] the penalty is imposed if there is date interception the penalty inflicted is Ugshs 5,000,000 or 12 months imprisonment or both fine and imprisonment. Here punishment as compared with International Law is left to the member state, the Convention never intend to punish criminals but creates only the offence under the cyberspace. Jurisdiction under the cyberspace is left to the member state after creating its own cyber law and other procedural law or rules.

Section 122[85] deals with fraud with dishonest intent while **Section 124**[86] deals with illegal access to computer system like in the Budapest Convention. **Section 123**[87] inflicts penalty to a person for interference of electronic communication to be a fine of not less than Ugshs 5 million or 2 years imprisonment or both fine and punishment. This is not the case to the Convention. If we can consider the Indian domestic law particular Section 43 of the *Information Technology Act*[88]. Which is national law of India creates a penalty like our law for damages for the computer and computer system. The criminal is liable to pay damages by way of compensation for the sum not exceeding 1 crone rupees to the victim.

Section 43 provides : If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network,

i. Accesses or secures access to such computer, computer system or computer network;
ii. Downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or

[84] Supra note 80
[85] ibid
[86] ibid
[87] ibid
[88] ibid

stored in any removable storage medium;

iii. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network

iv. Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programs residing in such computer, computer system or computer network;

v. Disrupts or causes disruption of any computer, computer system or computer network;

vi. Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

vii. Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there-under;

viii. Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

As Musinguzi,[89] pointed out, cybercrimes are intermingled with electronic commerce like e-signature, digital signature, digital devices and e-contracts and that they ought to have been addressed because they are very important. It is argued here that the legal regime in Uganda in respect of cyber fraud is still wanting and that EPOCA has not addressed all the issues in respect of cyber fraud, hence, inadequate because it leaves a big lacuna in the legal regime on

[89] **Musinguzii, A.J., op.cit.**

cybercrimes.

3.3 Conclusion

As observed above, detailed rules exist in relation to theft and frauds in paper -based transactions. It is noted that computer crime detection are a difficult task. Bringing the criminals to book becomes a formidable challenge since the laws in many countries have not kept pace with technology. Laws were originally designed to protect tangible assets and may not be sufficient to guarantee the protection of electronic bits of data. Given what has been discussed above the Ugandan legal frame work on cybercrime is fairly sufficient save for particular situations where it may need implementation.

CHAPTER FOUR
INTERNATIONAL LEGAL FRAMEWORK ON CYBER CRIME

4.0 Introduction

The purpose of this Chapter is to present a discussion on how cybercrime or cyber fraud has been provided for around the globe. It will show that the existing legal framework on criminal law has helped Uganda to counter cybercrime or cybercrime. It is doubtful whether the existing principles on criminal law designed to regulate paper –based transactions can apply to theft and frauds in on the internet and other electronic transactions. However, this point is being increasingly recognized as an area of concern and more and more countries are, therefore, enacting specific and comprehensive legislation to cover the acts of computer criminals.

4.1. Common standards: the Budapest Convention

The Budapest Convention was the first treaty aimed at enhancing the criminal justice, the treaty was to the effect of the following:

1. It criminalizes a number acts, or provides a list of attacks against and by means of computers.
2. Provides for procedural law implementations to enable the investigation of cybercrime and the acquiring of electronic evidence, in regards to any cybercrime more effective and subject to rule of law safeguards.
3. International police and judicial cooperation on cybercrime and e-evidence

The convention is available and open for ratification by any country prepared to implement it and engage with the rest of the states of have ratified it. By the end of the year 2016, which was marking the 15th anniversary of the Convention, more than 50 member States had codified the

convention and become Parties (European countries as well as Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and the USA). At the same time more than countries 17 from various regions of the globe had signed and signed it or had already been invited to ratify the convention.[90]

After the ratification of the Budapest convention on Cybercrime in 2001 by the majority of European countries, the Council of Europe commenced the aiding of other countries to ensure proper implementation of the treaty, first within Europe and thereafter by the year 2006 it was extended to other regions of the world, and in most cases it is in assistance with the European Union[91].

Nevertheless, by the year 2013 the entire matter had already been elevated to a different level. By February the year 2013, the United Nation Intergovernmental Expert Group made a resolution on the need for a wider treaty or convention regarding building as far as fighting cybercrime and enhancing cyber security is concerned.

Later in Seoul, the capital of Korea focus was turned to Global cyber space, where the conference was held in October 2013. As a result of the conference, the European Union together with the Council of Europe gained momentum on which the based to immediately execute their treaty on the joint project on Global Action on Cybercrime (GLACY). It was from this time that the Council of Europe decided to establish the popular known Cybercrime program Office with an aim to boost capacity building all over the world such as Romania, Bucharest and some parts

[90]Clough, Jonathan. "A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation." (*Monash UL Rev.* 40 (2014)

[91] Keyser, Mike. "The Council of Europe Convention on Cybercrime." (*J. Transnat'l L. & Pol'y* 12 2002)

of Africa including Uganda[92]. Whatever transpired from the Budapest Convention was operationalized by the International Cybercrime Treaty.[93]

4.2 The International Cybercrime Treaty:

4.2.1 Origins of Treaty

The Council of Europe refers to the union of 41 nations of Europe, which was established in May of 1949 in order to facilitate social and economic growth and foster unity among its members. It is headquartered in Strasbourg, France.[94] The Cybercrime Treaty has been the subject of much consideration by the European Union since as early as 1997. The goal of this treaty was viewed as an attempt to "harmonize laws against malicious hacking, virus writing, and fraud and child pornography on the net. It also aims to ensure that police forces in separate countries gather the same standard of evidence to help track and catch criminals across borders.[95] Since cybercrime often transcends a nation's borders in being committed, the measures to combat it must also be of an international nature.

Articles two through eleven of the Treaty accomplish the first goal of prohibiting specific types of conduct.[96] Each nation that signs the treaty is expected to outline certain mandatory criminal offenses and conduct and the related sanctions for crimes committed within that nation,

---

[92]Broadhurst, R. Developments in the global law enforcement of cyber-crime. *Policing: (An International Journal of Police Strategies & Management, 29*(3),2006).

[93] Ibid

[94] The Maudit Group. (n.d.). Glossary and Acronyms - International Business - Con to D. Retrieved January 14, 2007 from http://www.rmauduit.com/glossary-con.html.

[95] BBC News.. Cybercrime Treaty Condemned. (Retrieved January 2000, December 18) from http://news.bbc.co.uk/1/hi/sci/tech/1072580.stm.

[96] Global Lawful Interception Forum. (n.d.) Eight Reasons the US Should Ratify the Cybercrime Treaty. (Retrieved January 14, 200)7 from http://www.gliif.org/RafityNow/reasons.htm.

territories in their possession, on the nation's ships and aircraft, and by their citizens when they are abroad as foreign nationals.[97]

The offenses are broken down into four areas of crime, which are fraud and forgery, child pornography, copyright infringement (intellectual property), and system interferences, which affect network integrity and availability (covering many aspects of hacking). Due to objections by the United States, an additional provision prohibiting racist acts (e.g. distributing racist materials) on the Internet was kept separate of the treaty itself to be approved as its own protocol. The United States has not signed this protocol on the grounds it would violate freedom of speech.[98]

Articles sixteen through twenty-two of the Treaty accomplishes the second goal of ensuring the establishment of a national legal process for each country, including human rights safeguards, legal procedures, and the tools and procedures that will be used for criminal investigation.[99] Each nation must create specialized procedures for detecting, investigating, and prosecuting computer crimes and collecting any electronic evidence of the crime. Particularly of note, this provision includes the preservation of computer stored data and communications, system search and seizure, and real-time "wire-tapping" on the network.[100] The chief reasoning behind this section

---

[97] Ibid

[98] Archik, K, CRS Report for Congress. Cybercrime: (The Council of Europe Convention. Retrieved January 21, 2007) from http://fpc.state.gov/documents/organization/36076.pdf.

[99] Global Lawful Interception Forum. (n.d.) Eight Reasons the US Should Ratify the Cybercrime Treaty.

[100] Archik, K, CRS Report for Congress. Cybercrime: (The Council of Europe Convention 2004, July 22) .

of the treaty is the fact that cybercrime, and electronic communications in general, is generally fast, efficient, and hard to isolate. In order to obtain electronic evidence in a timely matter, the proper procedural tools and powers are needed to expedite matters so that the appropriate evidence can be secured.[101]

Articles twenty-three through thirty-five outline the third goal of creating an environment for international cooperation. It includes the areas where cooperation in cybercrime investigation is appropriate and also addresses the matters of confidentiality and the conditions of use.[102]

This last major provision establishes guidelines for extradition, collection of computer-based evidence in another country, and a 24x7 network that can provide immediate assistance in international investigations.

4.3 The council of Europe's Convention on Cybercrime

On November 23, 2001, the United States and 29 other countries signed the Council of Europe's Convention on Cybercrime as a multilateral instrument to address the problems posed by criminal activity on computer networks. Nations supporting this convention agree to have criminal laws within their own nation to address cybercrime, such as hacking, spreading viruses or worms, and similar unauthorized access to, interference with, or damage to computer systems.[103] It also enables international cooperation in combating crimes such as child sexual exploitation, organized crime, and terrorism through provisions to obtain and share electronic evidence. The U.S. Senate ratified this convention in August 2006. As the 16th of 43 countries to

[101] Ibid

[102] Global Lawful Interception Forum. (n.d.) Eight Reasons the US Should Ratify the Cybercrime Treaty.

[103] Supra note 98

support the agreement, the United States agrees to cooperate in international cybercrime investigations.

The governments of European countries such as Denmark, France, and Romania have ratified the convention. Other countries including Germany, Italy, and the United Kingdom have signed the convention although it has not been ratified by their governments.[104] Non-European countries including Canada, Japan, and South Africa have also signed but not yet ratified the convention."[105] In Uganda, this particular agreement has been signed by the government however, it has not yet been ratified or domesticated. The Treaty has to be put into practice by being ratified by the Ugandan parliament so that it can have the force of Law locally and the courts of law can be ably implement it.[106]

4.4 Mutual legal assistance treaty (MLAT)

A mutual legal assistance treaty (MLAT) is an agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.

Modern states have developed mechanisms for requesting and obtaining evidence for criminal investigations and prosecutions. When evidence or other forms of legal assistance, such as witness statements or the service of documents are needed from a foreign sovereign, states may attempt to cooperate informally through their respective police agencies or, alternatively, resort to what is typically referred to as requests for "mutual legal assistance."[107] The practice of mutual legal assistance developed from the comity-based system of letters rogatory, though it is

[104]Cyber Telecom: Cybercrime: International Treaty

[105] Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705, p. 14-15 (June 2007)

[106] Cryer, R. *An introduction to international criminal law and procedure.* (Cambridge University Press 2010).

[107] ibid

now far more common for states to make mutual legal assistance requests directly to the designated central authority within each state. In contemporary practice, such requests may still be made on the basis of reciprocity but may also be made pursuant to bilateral and multilateral treaties that obligate countries to provide assistance.[108]

This assistance may take the form of examining and identifying people, places and things, custodial transfers, and providing assistance with the immobilization of the instruments of criminal activity. With regards to the latter, MLATs between the United States and Caribbean nations do not cover U.S. tax evasion, and are therefore ineffective when applied to Caribbean countries, which usually act as offshore "tax havens"[109].

Assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. Some treaties may encourage assistance with legal aid for nationals in other countries.

Many countries are able to provide a broad range of mutual legal assistance to other countries through their justice ministries even in the absence of a treaty, through joint investigations between law enforcement in nations, emergency disclosure requests, letters rogatory, etc.[110] In some developing countries, however, domestic laws can actually create obstacles to effective law enforcement cooperation and mutual legal assistance. Many countries in the quest to ably implement International Corporation, they have resorted to Mutual legal assistance treaties

[108] Ibid

[109] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT/C/5/Add.32 30 June 2004) https://www.google.com/search?q=ohchr+uganda&ie=utf-8&oe=utf-8&client=firefox-b-ab

[110] ibid

whereby such countries help each other in executing legal procedures as far cybercrimes are concerned.[111]

In January 2000, the Government of Uganda decided to sponsor two draft conventions on extradition and mutual legal assistance prepared initially by UNAFRI. African delegates meeting in Cairo in November 1999 approved the draft. Fourteen countries, five African and international experts, OAU legal counsels and a representative of the United Nations Centre for International Crime Prevention attended. The contents of the draft convention on extradition covered comprehensive substantive provisions in the areas of principles of extradition, grounds for refusal of extradition, contents of requests for extradition and consideration of requests for extradition. The contents of the Convention on Mutual Assistance covers, inter alia, the scope of application, types of assistance, central authorities, contents of requests, execution of requests, refusal to offer assistance, return of completed requests and securing requested evidence.[112]

4.5 The Extradition Act Chapter 117

The Act in its appearance is a municipal law, but its contents clearly provided for the international frame work. Premised on that, I opted to lay it down as an international legal frame work due to the fact that it governs dealing with a criminal who is in another country.

Section 2, subsection (1), of the Extradition Act provides that "where an arrangement has been made with any country with respect to the surrender to that country of any fugitive or criminal, the minister may, by statutory case of that country subject to such conditions, [make] exceptions and qualifications as may be specified in the order, and this part shall apply accordingly";

---

[111] ibid

[112] The information submitted by Uganda in accordance with the consolidated guidelines for the initial part of the reports of States parties is contained in HRI/CORE/1/Add.69.

(b) **Subsection (2)** provides that "an order made under the preceding subsection shall recite or embody the terms of the arrangement and shall not remain in force for any longer period than the arrangement";

(c) **Subsection (3)** provides that "every order made under this section shall be laid before the National Assembly (Parliament)".

The challenge faced by the Government of Uganda at the moment is to put in place legal instruments that prohibit its relevant authorities from repatriation, extradition or expulsion of individuals who are in danger of being subjected to torture. According to the Extradition Act, section 3, the following provisions shall be observed with respect to the surrender of fugitive criminals:

(a) A fugitive criminal shall not be surrendered if the offence in respect of which his or her surrender is demanded is one of a political character or if it appears to a court or the Minister that the requisition for his or her surrender has in fact been made with a view to trying and punishing him or her for an offence of a political character;

(b) A fugitive criminal shall not be surrendered to any country unless provision is made by the law of that country, or by arrangement, that the fugitive criminal shall not, unless he or she has been restored or had an opportunity to return to Uganda, be detained or tried in that country for an offence prior to his or her surrender other than the crime for which the extradition is requested;

(c) **Section 10 (2)** of the Extradition Act provides that "The magistrate shall receive any evidence which may be tendered to show that the crime of which the prisoner is accused or

alleged to have been convicted is an offence of a political character or is not an extradition crime";

(d) **Section 11 (1)** provides that "In the case of a fugitive criminal accused of an extradition crime, if the foreign warrant authorizing the arrest of the criminal is duly authenticated, and such evidence is produced as subject to the provisions of this Act, would according to the law of Uganda justify the committal for the trial of the prisoner if the crime of which he or she is accused was committed in Uganda, the magistrate shall commit him or her to prison";

(e) **Section 11 (6)** provides that "Where the magistrate is not satisfied with the evidence mentioned in **subsection (1) or subsection (2)** of this section, he or she shall order the prisoner to be discharged";

(f) **Section 23** provides that "The Minister shall not transmit a requisition under **section 22** and a warrant shall not be endorsed under this part of this Act for the apprehension of any person if the offence is one of a political character or it appears to the Minister or a court that the requisition has in fact been made with the view to try or punish him for an offence of a political character."

The Extradition Act does not cover the aspect of torture and only covers cases of a political nature. The existing law on refugees is the Control of Aliens and Refugee Act and it permits arbitrary expulsions. However, it is generally agreed that the provisions in the Act are archaic and outdate and the policy of the Directorate of Refugees in Uganda is to use the 1951 Convention relating to the Status of Refugees and the 1969 Convention Governing the Specific

Aspects of Refugee Problems in Africa of the Organization of African Unity rather than this Act. There is a bill to repeal this law[113].

It is a main concern to the authorities of the Government of Uganda that there is no all-encompassing law to make torture a subject of extradition, deportation or return.

Over the past decade, it has been realized by all African States that there is a need to have efficient treaties and legislation on extradition and mutual assistance. The African countries realized that there was an expanding criminality, especially transnational criminality, which continued to threaten stability, security, peace and the development of societies.

In 1996, the United Nations Crime Prevention and Criminal Justice Division initiated the implementation of a project on extradition and mutual legal assistance in the African States. The project was implemented with technical cooperation and funding from the Departments of Justice and State of the United States of America[114].

UNAFRI is an organization based in Uganda. It is the African component of a network of United Nations-affiliated regional institutes for the prevention of crime and criminal justice. According to a survey by UNAFRI on extradition and mutual legal assistance in criminal matters, it was revealed that existing mechanisms, practices and legislation are inadequate and poorly developed. There is a dearth of bilateral extradition and the mutual legal assistance arrangements. However these are out dated and need to be replaced by modern arrangements.

---

[113] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT/C/5/Add.32 30 June 2004) https://www.google.com/search?q=ohchr+uganda&ie=utf-8&oe=utf-8&client=firefox-b-ab

[114]The information submitted by Uganda in accordance with the consolidated guidelines for the initial part of the reports of States parties is contained in HRI/CORE/1/Add.69.

The Act is important because even in circumstances where a crime has been committed online from a different country the provisions of the Act can be invoked and such a criminal is finally apprehended.[115]

4.6 Conclusion

As observed above, detailed treaties have been put in place to combat the escalating cybercrime around the globe. It is noted that computer crime detection are a difficult task. Bringing the criminals to book becomes a formidable challenge since the laws in many countries have not kept pace with technology. Laws were originally designed to protect tangible assets and may not be sufficient to guarantee the protection of electronic and online bits of data. It is often difficult to attribute guilt using the existing statutes since the act can be committed from a completely different jurisdiction.

[115] ibid

CHAPTER FIVE

FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter presents a summary of conclusions and recommendations of the study. It is hoped that the recommendations presented here will contribute to future making of policies geared towards combating cybercrime in general, and in particular, cyber fraud in the urban informal sector. These recommendations have been drafted to contribute to the challenge of halting social trends that result into the growth of cybercrime.

5.1 FINDINGS

The research findings also indicated that despite the existence of national, regional and international laws on cybercrime/ fraud, there was a general lack of enforcement and implementation of the legislation. This further facilitated a breeding ground for the phenomenon of cybercrime/fraud.

Further, from the findings, there was a general wave of indifference among members of the community and the state. The fact that a legal framework was in place, little had been done to enforce it. On the other hand, the fact that the community looked at cybercrime as a positive investment, that is to say, technological development and thus overlooking its negative implications, little was done to report such cases and to deter from providing employment opportunities to such criminals.

On the side of the criminals, ignorance of the law further facilitated cybercrime and given the fact that people were highly 'invisible', addressing the problem of cybercrime was far from over. The factors that have facilitated the persistent increase of people to participate in urban informal

activities that have been mentioned in the preceding paragraphs are further classified and elaborated below;

5.1.1 Deficiency of a Body of Ethical Principles

The research results indicated that the Department of Labour Employment and Industrial Relations in the Ministry of Gender, Labour and Social Development lacks a body of ethical principles against cybercrime. Notwithstanding the presence of criminal laws in Uganda, such ethical principles are deficient in that important organ of the state of Uganda.

5.1.2 The Lack of Political Will

According to the research findings, it was noted that there was generally an increase in the number of young people in cyber fraud with the magnitude in the urban informal sector alone estimated at over 2 million. Cyber fraud forms in Uganda depicts white collar crimes and the level of criminology and an immoral/unethical society we live in, a society which has been defiled and everyone does not trust the internet and any electronic transaction. The prevalence of cybercrime and cyber fraud points to utter disrespect of national and international laws, treaties and conventions and the lack of political will to implement them.

5.1.3 Ineffective Education Programmes

Despite the introduction of the Universal Primary and Secondary Education Programmes in 1997 and 2007 respectively, it has been noted in the research findings that there are many children not enrolled in schools. The main reasons for this disorder are; the lack of school fees and the lack of scholastic materials, on the side of the parents, which has led to several drop outs who have gone looking for survival elsewhere hence end up into crimes.

Though we can acknowledge that Universal Education increased the Net Enrolment Ratio to approximately 50% (DFID, 2010), the challenge that accrued out of this entailed limited

facilities in terms of classrooms and the lack of teachers which later on led to child school dropouts. This spells out a deficiency in our education system, since even the newly introduced USE has not helped much in attracting more students with equipping them with ethics and morality.

5.1.4 Poor Implementation of the Laws against crimes and Policies in the Country

Uganda has enacted and ratified many policies and laws at the national and international level, but many of them have not been implemented to address the problem of cybercrime/cyber fraud in the country. The limited implementation of these policies and laws including; the The Extradition Act Chapter 117, the Budapest Convention, The International Cybercrime Treaty and The International Cybercrime among others. Spells out the increased magnitude of cyber fraud cases in the country. Most of these laws are therefore redundant since they have not been implemented to address the problem of cybercrime.

5.1.5 The original laws enacted did not cater for the new forms of cybercrime and electronic transactions.

According to the research findings, it was noted that there are criminals penal aimed at controlling fraud and any person from getting involved in fraud. However, household poverty was the major cause of children's participation in the labour force. It was noted that children worked to supplement meagre family incomes and most of them did not attend school since they could not afford school fees and scholastic materials.

Poverty as the major underlying cause of crime exists in almost all traditional settings in Uganda. It is true that the poorest most disadvantaged sectors of the society constitute the vast majority of criminals, since such people seek salvation from poverty through any means. Cyber fraud can

therefore not be eliminated unless poverty has been earnestly addressed, and harmonising the existing mechanisms with ethical principles.

The persistent increase in the problem of cyber fraud therefore explains something more than just a policy and legal framework. The government being the supreme body that is obliged to protect and promote its citizens, the government through the Ministry of justice, should shoulder the mantle to uphold a crime free environment through the initiation of effective policies with ethical principles therein as well as their implementation.

5.2 Recommendations

Based on the findings of the study in regard to protection and promotion of the welfare of the Ugandan citizens, the study gave a way forward and accordingly, the recommendations that were developed from the study which includes;

5.2.1 A Body of Ethical Principles against cybercrimes

Earlier on in the background of the study (Section 1.2), we noted that the main organ of the state responsible for matters regarding crimes in Uganda is the ministry justice and Constitutional Affairs. This organ should compose, subscribe to and educate the population about a body of ethical principles against cybercrime.

a) Composing the Ethical Principles

The Ministry of justice and constitutional affairs should compose a set of ethical principles which are in accordance with internationally, regionally, nationally and socially recognized or accepted criminal justice system. Such ethical principles ought to be derived primarily for the benefit and protection of society and the economy where the possibility of endangering the population exists.

b) Subscribing to the Body of Ethical Principles

It is suggested that all employers in the formal and informal sectors should be legally led towards recognising that they are ethically responsible to the public and the economy who are potential victims or donors of cybercrimes/ cyber fraud. Such employers ought to subscribe to the above mentioned Body of Ethical Principles once it is put in operation.

c) Educating the Ugandan Population about the Role of Ethical Principles against cybercrime

The above given Department of Labour Employment and Industrial Relations should be charged with the duty of educating the population about the benefits and protection the Body of Ethical Principles offers.

5.2.2 The Political Will to Enforce Laws

Acknowledgement of cyber fraud as a problem by the government of Uganda should be a **significant move and considered paramount in addressing the problem of cyber fraud in Uganda.** Cybercrime/ cyber fraud should be criminalised and massive awareness about the law by those in authority through print and electronic media should be done in all sections of society and included in development plans.

a) Supportive National Political, Legal and Institutional Framework

There is need for political commitment to ensure that cyber fraud is mainstreamed into broader development plans and programmes. For instance, integrating cyber fraud as an explicit concern in the Millennium Development Goals and Education for all plans, poverty reduction strategies and criminal justice consistent with international child labour standards,

is necessary both as a statement of national intent and as a legal and regulatory framework for efforts against cybercrime.

As cyber fraud is an issue that cuts across different sectors and areas of ministerial responsibility, progress against it requires that institutional roles are clearly delineated and that effective coordination and information sharing structures are put in place.

5.2.3 Increase Budgetary Allocation to Government Institutions

It was observed that the major government institutions – Uganda Police Force (CFPU) and the Ministry of justice and constitutional affairs had limited financial resources to foster their activities against cybercrime. Government should increase this funding so that these institutions execute their duties as mandated by the law.

Public accountability of the allocated funds should be done as a matter of fact, and monitoring and evaluation of programmes done by an independent institution from the state. On the side of the institutions, budgetary allocation should give priority to address cybercrime in the urban informal sector.

5.2.4 Stakeholder collaboration

Different institutions have worked hand in hand with the state to address the problem of cybercrime. These include; international organizations, CSO's and NGO's. In order to fully address the challenge of cyber fraud and therefore to promote the wellbeing of the population and protect the economy, multi-stakeholder collaboration is vital. Legislators, civil society, academicians, researchers, the international community, educationists and the community should jointly develop and implement effective and efficient preventive measures if the welfare of the economy is to be guaranteed and their rights upheld.

5.2.5 Revise Universal Education Programme

Education is a constitutional guarantee under Article 34 (2) of the 1995 Constitution of the Republic of Uganda; thereby it is stated that: A child is entitled to basic education which shall be the responsibility of the state and the parents of the child. Ironically, many students especially in the rural areas and urban outskirts have not been able to go to school because of household poverty. This constitutional establishment by the government of Uganda is not enough to argue that every child has a right to education, when they do not have sufficient means for its implementation. Revision of education programmes to suit today's challenges is vital if criminology is to be addressed. This can be done through;

a) **Enforcement of Compulsory UPE**

The researcher is of the view that primary education should be completely free, universal and compulsory to every child in the family and should not only be restricted to poor children. UPE should encompass comprehensive policies indicating the current percentage of GDP allotted to basic education and a target percentage for future allocations and plans for improvement of education in coverage, quality and relevance. UPE should be made more attractive to the learners so as to minimise child dropouts (increase retention) and facilities should be provided as well.

While we can applaud the government for introduction of the USE, it is sad to point that those that have dropped out before completion of the primary level cannot proceed to the secondary level. It is therefore important to address the several challenges at the primary level to fully attain the goal of universal education. It would reduce on the amount of idle minds and the rate at which people engage themselves into criminal activities.

b) Establishment of Community Polytechnics

These will enable access to vocational training and education for primary school dropouts. These polytechnics need to be made more accessible, well equipped and attractive to children and parents. These children should also be provided with tailor made skills especially those in the urban informal sector. These will enable the children gain experience and therefore earn a decent income for survival. It reduces unemployment and hence people be involved in productive work.

Other recommendations that are not necessarily in line with the objectives have been listed and these include;

5.2.6 Implementation of a strict criminal justice in the Country

To be able to create a country free of cybercrime and its dangers, the aforementioned laws (3.) have to be implemented as a mandate for the welfare of the child. With proper guidelines, these laws have to be translated into various vernaculars for easy interpretation by the citizens of Uganda. Institutional organizations and the Government of Uganda with support from the international community should then sensitize the general public right from the grassroots level about the laws and policies on cybercrime. This will put them in position to report cases of to those in authority.

5.2.7 Poverty Reduction

The Government of Uganda should create and implement an explicit policy on poverty alleviation, which may include the enforcement of socioeconomic policies to promote economic growth. Uganda has for the fact poverty alleviation programmes like the "prosperity for all" but these have specifically targeted the rural setting and ignored the urban setting. The urban sector

should be put to consideration in these programmes to target its poor communities especially those in the informal sector.

5.3 Further Reading

Although the study has been exhaustive, the researcher recommends further studies on the phenomenon of cybercrime given the very dynamic society we live in. Studies should be conducted to ascertain why, despite concerted efforts in terms of policy and legal interventions, cybercrime is on an increase. The studies will not only widen the knowledge base, but also provide a viable way forward.

5.4 Conclusions

Given the research into the correlation between cyber fraud and the legal frame work in place, it is apparent that cybercrime/ cyber fraud is on an increase every day, and was estimated at a magnitude of over a cases million. Although more young people participated in various activities of crime, it was observed that all the culprits worked in order to earn a leaving and for survival. The lack of family income, and or its inadequacy explained the major reason why most young people lacked school fees. Young people get engaged in different criminal activities hence exposing themselves to chances of participating cybercrime/cyber fraud.

BIBLIOGRAPHY

APACS, 2008; FPEG, 2009; European Commission, 2008. (*JIBC publishing December 2009, Vol. 14, No. 3)*

Archik K, CRS Report for Congress. Cybercrime: The Council of Europe Convention. (2004, July 22) Retrieved January 21, 2007 from

Bajaa K. K. & Debjani N, "Fight against payments fraud: The target is moving, but no everybody takes aim' (published 2011 by Sky media)

BBC News, Cybercrime Treaty Condemned. From (2000, December 18) http://news.bbc.co.uk/1/hi/sci/tech/1072580.stm.

Brainbridge, D. , "Introduction to Computer Law, Pearson, Education London , (5th Ed, 2004)

Broadhurst R, Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, (*29*(3), 408-433

Cap. 16 Vol. 1 of the laws R.E. 2002).

Comer , M.J. , Corporate Fraud, Mc Graw Hill Book Company, (2nd Edn, London 1985 pg 40).

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT/C/5/Add.32 30 June 2004)

Criminal Case Number 137of 2012 between the Republic and Hassan Ndanijagira @ Natukunda. (The records were published at the Mbarara High Court on 20 June, 2013).

Criminal Case Number 89 of 2009 at Kampala Resident Magistrate's Court. Records in respect of this file were accessed by the Researcher during the Field Survey

Cryer R, *An introduction to international criminal law and procedure*. (Cambridge University Press 2010)

Cyber Telecom: Cybercrime: International Treaty

Daid L.C, Computer crimes categories: How Technology Criminals operate, (Michigan state University, East Lansing Michigan 2012)

Gavazos, E. A., *Cyberspace and the Law, (*Cambridge-London, 1996, p. 1)

Gibbons, J. H., "Selected Electronic Funds Transfer Issues: Privacy, Security, and Equity", U.S. Government Printing Office, Washington, D.C. 20402.

Global Lawful Interception Forum. (n.d.) Eight Reasons the US Should Ratify the Cybercrime Treaty. (Retrieved January 14, 2007)

Global Lawful Interception Forum. Eight Reasons the US Should Ratify the Cybercrime Treaty (2009).

Gunarto ,H., Ethical Issues in Cyberspace and IT Society Ritsumeikan Asia Pacific University

Heathcote,P.M., (ICT,Payne-Gallawary Publishers,Ipswish,2008)

Joseph Migga Kizza, "Ethical and Social issues in the information age" second edition, springer, (2003).

Kaspersky Security Bulletin (2014). http://securelist.com/files/2014/12/Kaspersky-Security-(Bulletin-2014-Malware-Evolution.pdf)

Keyser, MThe Council of Europe Convention on Cybercrime. *J. Transnat'l L. & Pol'y*, *12*, 287. (2002). .

Kondobagil, J, *Risk Management in Electronic Banking; Concepts and Best Practices*, John Wiley & Sons (Asia), Pte Ltd: (Singapore, (2007) at p. 21).

Lloyd, I. J., Information Technology Law, (Butterworth 3rd Edn, London, 2000 pg 1

Lloyd, I. J., *Information Technology Law,* 6th ed, (Oxford University Press, 2011, p.210)

Loudon, C.K. & Traver, C.G., *op.cit.*, at p. 257).

Loudon, K. C. & Traver, C.G., E-Commerce: Business, Technology and Society, (4th Edn, 2008, Person Education International, New York, p. 257).

Mambi, A., shaping the information society, e-children protection, legal measures, a paper presented at IGF, (2nd Parliamentary Forum 2013)

Masadeh, A. M. S, Combatting Cybercrime: Legislative Approach: A comperative analysis between Quatar, UK and UAE (2012).

Prasana, A., "Cybercrime: Law and Practice" accessed at

Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705, p. 14-15 (June 2007)

See Criminal Case No. 518 of 2010 pending before the Ilala District Court in Kampala. Records in respect of this case were accessed by the Researcher during the Field Survey at the Ilala District Court, Kampala on 8th July, 2013.

See the particulars of offence in Criminal Case No 147 of 2009.

Sigh, N. P., "Online Frauds in Bank with Phishing" *Journal of Internet Banking and E-Commerce, (*August 2007, Vol. 12, no. 2).(http://www.arraydev.com/commerce/jibc/)

Singh,Y., ''Cyber Laws,'' 5th Edn,New Delhi: Universal Law Publishing Co. (Pvt.Ltd., 2012)

Ssentogo R., " Legal Implications of Developments in Information and Communication Technology: An Appraisal of the Electronic and Postal Communications Act, (2010 in relation to cybercrimes in E-Commerce in Uganda")

Symantec Global Internet Security Threat Report: Trends for 2009 Volume XV, (Published April 2010)

Talwar, S. P. "Computer Crime - an Overview" (daily newspaper called Habari Leo of 28th August, 2008) Accessed at http://rbidocs.rbi.org .in/rdocs/Bulletin/DOCs/6270.doc

Technology" The Uganda Law Reform Journal, ()Vol 2, No.1, 2009, pg.21

The Maudit Group. (n.d.). Glossary and Acronyms - International Business - Con to D. (Retrieved January 14, 2007) from http://www.rmauduit.com/glossary-con.html.

The Uganda police Annual Police crime and traffic report of 2013

The Uganda police Annual Police Report of 2014

The Uganda police Annual Police Report of 2015

Ubena, J. "Why Tanzania Needs Electronic Communication Legislation? Law keeping up with

Uganda (2016 crime and safety report).

Virus Bulletin Conference, (September, 2009)

Viswaanathan , A., Cyber Law, Indian and International Perspectives on Key Topics Including Data Security, E-Commerce, Cloud Computing and Cybercrimes, Lexis Nexis (Butterworth Wandwa, Nagpur, 2012)