DEGREE PROJECT

TELECOMMUNICATION FRAUD PREVENTION POLICIES AND IMPLEMENTATION CHALLENGES

DOMINIC AYAMGA

Information Security, master's level (120 credits)
2018

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ UNIVERSITY OF TECHNOLOGY

Acknowledgement

First of all, my greatest thanks goes to YAHWEH for having seen me throughout my education.

My thanks and appreciation go to all the lecturers and management of Luleå University of Technology and the Department of Computer Science, Electrical and Space Engineering for their tireless efforts in impacting knowledge, training and grooming me, most especially my supervisor Professor Tero Päivärinta and Dr. Diana Chroneer for the patience and guidance throughout my thesis.

I also wish to thank and show my appreciation to the following people whose tireless effort made it possible for me to pursue my master's program, without whom I could not have afforded the cost of a master's programme, the management and entire staff of GetFund, Professor Thomas Mba Akabzaa, Hon. Moses Asaga, Hon. Dr. Dominic Akuritinga Ayine, Hon. Boniface Gambila, Dr. Gilbert Ayimbire Abonuusum and to my sisters, Esther Anapoka Ayamga, Francisca Azaarebuno Ayamga, Christiana Anapogbila Ayamga and my late sister Lydia Ayampoka Ayamga.

Further, I sincerely wish to thank Dr. Gilbert Ayimbire Abonuusum and Dr. Daniel A. Ayoung for reviewing my thesis for me.

Last but not the least, I thank Mr. Morrison Davie and colleagues, I am grateful to you all for the support and time spent with you.

Abstract

The telecommunication system has being one of the greatest inventions of man. Ever since its introduction, it has grown to become the backbone of development and a platform for good governance for most countries throughout the world. Sadly, this good invention of man was never designed with its security or the security of its services in mind [22]. Despite the importance of telecommunication, and the existence of telecommunication systems for so many years, telecommunication system security are neither well understood nor managed effectively [22]. After several years of telecommunication system existence, security concerns are becoming a threat to its existence and operations.

All countries have policies regulating telecommunication operations as well as policies to ensure sanity in the use of telecommunication platforms to the benefit of their societies, governments and the telecom operators. The challenge however, is how efficient and effective these policies are implemented. These challenges, create room for criminals to commit fraud using telecom platforms by exploiting the weaknesses in either the policies or the lack of will to implement the policies by regulators.

This thesis used field research method to examine the existing telecommunication fraud prevention policies, the current challenges in implementing these policies and the existing telecom frauds. Using the country Ghana as a case study, the current challenges were broadly placed into three (3) categories as follows: (a) regulators challenges, (b) operators challenges and (c) User/subscriber challenges.

Unlike findings of previous studies, the research found that: (i) inefficient telecommunication fraud prevention policies, (ii) the quest to earn high revenue in international termination fees to sustain the economy and telecom operations and (iii) lack of proper coordination and cooperation between implementation agencies, are the new challenges which were not previously stated as challenges to the implementations of telecommunication fraud prevention policies. This does not discount the fact that some of the previously revealed challenges persist.

The research findings are used to generalised for other developing countries with features similar to Ghana especially sub-Sahara African countries. And also, all the recommendations are applicable as well.

Table of Content

List of Tables

List of figures

Abbreviations

CFCA	**C**ommunication **F**raud **C**ontrol **A**ssociation
L.I	**L**egislative **I**nstrument
SIM	**S**ubscriber **I**dentification Module
AML/CFT	**A**nti-Money **L**aundering/**C**ombating **F**inancing of **T**errorism
FATF	**F**inancial **A**ction **T**ask **F**orce
NCA	**N**ational **C**ommunication **A**uthority
NITA	**N**ational **I**nformation **T**echnology **A**gency
CID	**C**riminal **I**nvestigation **D**epartment
ID	**I**dentification
INTERPOL	**I**nternational **P**olitical and **E**conomic **O**rder **L**eaders
NCCE	**N**ational **C**ommission for **C**ivic **E**ducation
UNECA	**U**nited **N**ations **E**conomic **C**ommission for **A**frica
ITU	**I**nternational **T**elecommunication **U**nion
WTO	**W**orld **T**rade **O**rganisation
CP	**C**ut and **P**aste
TMA	**T**ake **M**odify and **A**pply
BoG	**B**ank of **G**hana

Introduction

Telecom policy (just as any public policy), is defined by James Anderson as a "purposive course of action or inaction undertaken by an actor or set of actors in dealing with a problem or matter of concern" [1]. Most public policies are influenced by politics. According to Deborah Stone, many components of public policy process are sometimes not based on national analysis but are instead highly political [2], [3].

Policies on telecommunication, such as fraud prevention telecom policies are part of or form a component of governments' horizontal policies throughout the world. "A horizontal policy is a policy developed by two or more organizations, each of which has the ability or mandate to deal with only one dimension of a given situation" [4]. Governments are increasingly focusing their efforts upon horizontal policy-making in recognition of the fact that many of the objectives they seek to achieve are complex and relate to the mandates of two or more departments, jurisdictions or non-governmental organizations [4].

Most governments throughout the world have a telecom policy requirement or vision of a universally available, affordable and quality telecommunication services provided through open, competitive, and well managed markets and ubiquitously adopted to the benefit of their economies and societies [5], [6], [7], [8]. This policy incorporates the concepts of Universal Service (US) and Universal Access (UA). Universal Service refers to telecom services offered at the individual or household level while Universal Access refers to telecom services offered at public shared level [9], [10], [11], [12], [13].Despites the importance of telecom policies, just as any other public policies, policies on telecommunication and for that matter, fraud prevention telecom policies are not without implementation challenges. These challenges include, corruption, weak institutions and lack of skilled man power [14].

Information Technology has penetrated every sector of our lives in recent times, and so are the activities of the fraudsters. Fraudulent activities have occurred in many areas of our daily lives such as telecommunication networks, mobile communications, online banking, and Ecommerce to name just a few.

Individuals, governments, and businesses incur significant financial loss through telecom fraud. And as a result, fraud prevention and detection has become an important issue to be explored. Fraud is a continuous battle with ever changing rules of engagement, and therefore effective fraud management requires a specific mind set, approach and strategy [15]. This is very challenging for individuals, security/information security personnel, businesses and governments alike, as it comes with greater cost.

In recent years, the telecoms industry has witnessed more well organised and financed criminal gangs operating across international boundaries who target specific telecoms services to maximise their revenues [15]. "Some of the most deftly perpetrated offences with or against telecommunications systems are never detected, not even by their victims. Of those which are detected, some are concealed from authorities because disclosure could prove embarrassing or commercially inconvenient to victims" [16].

Governments throughout the world encounter varying degrees of challenges in implementing telecommunication fraud prevention policies ranging from lack of technical infrastructure, weak financial strength to lack of political will.

While most developed countries have been able to eliminate some of these challenges leading to a decline in telecom fraud rate, third world or developing countries are still battling with even the most basic challenges in creating/designing and implementing telecommunication fraud prevention policies. Thus, there is a wide spread of telecom fraud and their inability to prevent or detect most of them. This thesis assesses the current implementation challenges of the telecommunication fraud prevention policies vis-à-vis fraud rates in developing countries using Ghana as a case study.

1.1 Motivation

The Ghanaian government just as most governments throughout the world are in a continuous battle with fraudsters in the field of telecommunication and its related sectors [83], [84], [85], [86]. A battle in which the fraudsters seem to have an upper hand as they always seem to be a step ahead of governments/regulators and operators due to their unpredictability [15].

The quest to contribute in identifying the root causes of most telecom fraud by looking into the current challenges in implementing telecommunication fraud prevention policies vis-à-vis the rate/level of telecom fraud in developing countries and make recommendations to augment governments/regulators and operators efforts in combating telecom fraud has been the motivation in carrying out this research. A security policy is the blue print of every security architecture and hence the root security of every infrastructure. An ineffective/weak security or poor implementation of an effective and robust security policy is a root cause of security failure/breach.

After perusing several relevant literature, it was detected that, most literature are directed towards specific problems or specific areas of telecom fraud (example simbox fraud) which is consider as tackling the symptoms and not the root causes of telecom fraud. There are some literature [40], [89], [90],[91] which attempts to tackle telecom fraud and its related cyber fraud from the policy level which is very fundamental to tackling the telecom fraud. This thesis considers telecommunication fraud prevention policies inefficiencies as the root sources of telecom/cyber fraud. Hence the motivation to undertake a research on Telecommunication Fraud Prevention Policies and Implementation Challenges.

Due to the security sensitive nature of the area of research, the only viable research methods capable of extracting data from regulators and operators is field research [22]. Besides field method, regulators and operators often do their own internal researches which in itself is a form of field research. The reason is, regulators and operators need to trust, have guarantees/assurances or physical knowledge of researcher in order to work with them. Moreover, physical observations are necessary since the area of research also includes behavioural analysis. These can only be achieved through field study [22].

The closest method beside field method is based on published field studies, that is, literature review which is considered an applied method. This however, is very difficult considering the fact that there are only few publications regarding this area. Again, the content published are often being regulated by regulators and operators. Moreover, it is highly unlikely for a researcher to obtain the current challenges facing telecommunication fraud prevention policies implementations by reviewing previous literature [22].

An alternative besides field study will deprive the researcher of observation of behaviour which is a critical part of the research area. Again, the margin of error will be very large

using a different research method besides field study method thereby reducing the reliability and credibility of the findings.

The field of telecommunication is a closed system [22]. Hence it is very difficult to obtain data due to issues of privacy and other security related issues. Even with the field study, only limited data may be given to the researcher(s) and researchers may even be asked to sign a bond to a non-disclosure of results or findings [22]. This closed nature of the telecommunication industry makes it necessary to have access to the inner circles to be able to have any meaningful research on the telecom industry and its related sectors.

1.2 Research Problem/Problem Statement

All countries have policies regulating telecommunication operations as well as policies to ensure sanity in the use of telecom platforms to the benefit of their societies, governments and the telecom operators/companies. The difference however, is how effective these policies are and how efficiently and effectively these policies are implemented. These differences create room for criminals to commit fraud using telecom platforms by exploiting the weaknesses in either the policies or lack of will to implement the policies by regulators.

Telecommunication fraud, mostly considered under a broader context as Cybercrime, though rightly placed, makes it difficult to isolate it and deal with it as a specific problem in most public discussions and in literature. Again, most of the frauds perpetrated by the fraudsters or cyber criminals are similar to what is being committed in the telecom industry but with slight variations.

In the telecom industry, companies are also involved in defrauding governments or states. This is done by way of tax evasions [33]. Telecommunication Service Providers also engage in slamming (when phone carriers illegally change customers' telephone service without their permission [22], [50]) and cramming (when phone carriers illegally add charges to customers' telephone bills for services they did not authorize. Customers are often deceived into accepting these charges while signing promotional materials or through social engineering techniques like negative option marketing [22], [51]) frauds thereby defrauding subscribers [14], [35], [36], [37]. Telecoms fraudsters are becoming more innovative in their techniques, the services and products they target. Communication Service Providers sometimes forget that highly organised fraudsters are actually running their own business and have their own "customers" [15].

Despite the decline in the percentage figure as reported by the Communications Fraud Control Association (CFCA) survey in 2015, the actual financial, informational and reputational damage to countries, telecom companies and other businesses as well as individuals is still huge and has had a serious negative impact globally [32].

The main challenges in Ghana and other developing countries in handling telecommunication frauds and subsequently cyber frauds are policies, technology and the political will to enforce or implement these policies [2], [14]. The policies on telecommunication frauds or cyber frauds are either not thoroughly thought through, inefficient or not enforced by successive governments [14]. This is because Information Security is often not considered a priority at both the parliamentary and the executive levels of successive governments and hence Information Security is often an afterthought which is often reactive and not proactive [14].

For instance, there has been an insufficient policy on telecom fraud as stated in the Consumer Protection Section and Fraud Prevention, Privacy Protection Subsection of the National Telecommunication Policy (2005) as presented by the Ministry of Communication stipulating how the National Communication Authority (NCA) handles telecom fraud and how it is to be handled if committed [5].

Even though in section 41 of the National Communication Authority Act 1996 (Act 524) on National Communications Regulations, 2003, L.I., 1719 [38] outline some procedure to be used to settle disputes between subscribers and operators, it does not cover much and does not explain in details what kind of frauds are covered. What is worse is that, not much education is given to the citizenry of the existence of such an act of parliament. This makes most Ghanaians unaware, very vulnerable and unable to address frauds related to telecommunication.

During a pre-research prior to the research, it was observed that, most organizations and institutions often take little consideration into security during designs of new information systems. A clear example is the recent software system designed to print out the pay slips (e-slips) of all workers under the Controller and Accountant General Department online. Though the system incorporated the use of passwords, one major thing missing was education for the employees most of whom (especially those in the villages) do not even know how to use the internet left alone understanding the essence of passwords. Not keeping your password secrete is same as not using a password. The lack of security awareness education on keeping the passwords secrete to employees by authorities makes these employees vulnerable to identity frauds [20].

Most of these security vulnerable employees often give out their usernames and passwords to internet cafè attendants to print out their pay slips for them. Some give out their usernames and passwords by writing them on papers or mentioning them out to the internet cafè attendants without taken notice of who is also listening or will have access to their usernames and passwords, considering the fact that the main operation centres for most cyber fraudsters in Ghana are in the internet cafès. The security risk here is that, a fraudster having access to the usernames and passwords will be able to know the salaries of employees and can printout employees pay slips and use them to perform fraudulent transactions like hire purchases or even loans on behalf of unsuspecting employees since most businesses and banks only require credible pay slips to grant loans or for hire purchases.

Another area exposing the lack of political will to enforce Information Security policies in Ghana is the SIM Card registration exercise. An exercise conducted under the Subscriber Identity Module Registration Regulation, 2011, L.I., 2006 of the parliament of Ghana [39]. This does not only expose the lack of political will to enforce its implementation but goes to explain the fact that Information Security is not a priority at both the parliamentary and the executive levels of successive governments of Ghana. This can be explained by the fact that much education was not given to the people on the essence of the SIM Card registration exercise.

The authorities could not prevent the use cards deemed as not valid (example the use of the national health insurance cards for sim card registration) to register their sim cards [88] as holders of those cards were not subjected to thorough screening prior to their issuance. Again, it is easy in Ghana to use either a family member’s or friend’s Voter Identification Card to

register your SIM Card. The worse is even that, the various telecom operators do not even educate their own employees (merchants) on the essence on the SIM Card registration exercise as it a common practice to see their employees (merchants) selling both pre-registered SIM Cards and unregistered SIM Cards. The questions now are; with whose Voter's Identification Cards are those pre-registered SIM Cards registered? Will a fraudster opt for an unregistered SIM Card instead of the pre-registered SIM Card? How easy will it be to trace a fraudster using a pre-registered SIM Card not in his/her name?

This is attested to when the National Communication Authority (NCA) advised subscribers to re-register and admitted that even though Ninety-Five (95%) percent had registered, majority did not register with valid Identification Cards (IDs) [40]. This thus, defeats the purpose of the "Know Your Customer (KYC)" procedure which requires operators to document and verify subscribers' identities which enables operators to combat crime, fraud scheme involving mobile phones and money laundry [40]. This is similar to what is required of banks, insurance companies, casinos as part of the framework of international Ant-Money Laundering/ Combating Financial Terrorism (AML/CFT) set by the Financial Action Task Force (FATF) [40]. This also violates Anti-Money Laundering Act, 2008, Act 749 of the Parliament of Ghana enforceable by Bank of Ghana, "an act to prohibit money laundering, establish a Financial Intelligence Centre and to provide for related matters" [41].

The **Mobile Banking fraud**, the mobile banking system introduced by the Bank of Ghana (BoG) has had a wide adoption by most Ghanaians for its ease of conducting banking transactions outside the traditional banking premises, for the fact that it's available anywhere within the country Ghana and its transactions are possible 24/7 [87].

This good business model however, was not given much security consideration (physical security and education) during its conceptualisation and implementation stages. Not much consideration was given to educate the citizenry or to create security awareness of the citizens and also, on the physical security of mobile money merchants before rolling out the mobile banking system (**mobile money)**. This has worsen the security plight of citizens as both customers and merchants are facing daily robberies from the so called **"GAME BOYS"** and other armed robbers both through social engineering and physical attacks respectively [88].

The Ghana Chamber of Telecommunications confirmed that, a total of Two Hundred and Seventy-eight (278) mobile money fraud cases were recorded in 2015 and Three Hundred and Eighty-eight (388) mobile money fraud cases in 2016 [88]. These figures represents just less than twenty percent (20%) of the actual fraud incidents associated with mobile money in Ghana. Majority are not report as a result of lack of trust of authorities and people not knowing whom to report to.

The head of Research and Communications at the Ghana Chamber of Telecommunications and the manager of Mobile Finance Services Analytics, Budget and Reporting at MTN mobile money both alluded that some customers are not aware of the existence of mobile money fraud in Ghana because of limited information, publicity and inadequate customer vigilance and compromises as some the contributory factors to the rise of mobile money fraud in Ghana [88].

Bank of Ghana, the main regulator of the mobile banking or mobile money only attributed rise in the mobile money fraud to the overwhelming growth in mobile money

wallets/accounts [88]. Mobile money merchants on the other hand, blame the rise of mobile money fraud in the Ghana on customers' greed and ignorance [88].

For instance, given the fact that the mobile banking system procedure cannot guarantee end-to-end security, taking into consideration the fact that mobile phones have low computing power and hence with much weaker encryption algorithms makes the mobile banking process susceptible to Man-In-Middle attacks, sniffing and spoofing attacks, social engineering attacks [72], much education and security awareness needed to have been given to subscribers as to how to minimize the possibilities of these forms of attacks.

As a result of the above, most institutions in Ghana are in a much weaker position to handle telecom or cyber fraud in Ghana. Again, the Ghana Police Service are not properly equipped logistically as well as not well trained to effectively and efficiently crack down telecom or cyber frauds in Ghana. Hence the inefficiencies of the police and the wide cyber or telecom frauds in Ghana.

From the report of the United Nations Economic Commission for Africa on tracking illicit financial flow in African countries (UNECA 2015), the government of Ghana reported that SIM box fraud has cost $5.8 million in stolen taxes alone [33]. That is even only what is lost through SIM box fraud, what of what is lost through Social Engineering via fraudulent text messages and calls from fraudsters to innocent hard working Ghanaians? What of money lost through over subscriptions charges on Ghanaians? What of the greater percentage of fraud incidences not reported, not because the victims do not want to report but because they do not know the institution to report to?

From the report [33], it appears that whatever is happening in Ghana relating to the prioritization of Information Security at both the parliamentary and the executive levels runs through most of the African countries as it reflects in the massive losses incurred as a result of SIM box frauds in the various countries. However, this thesis only focuses on Ghana.

Perhaps the unprecedented cyber-attack which took Liberia's entire internet down on November 4, 2016 and most recently, the "WannaCry" malware invasion worldwide on May 12, 2017 should serve as a lesson to the Sub Sahara African countries and the rest of Africa to consider Information Security as a priority at both parliamentary and executive levels. The general impression is that policy makers and implementers are several steps behind in comparison with fraudsters operations or activities.

After reviewing several literature related to telecommunication fraud prevention policies, the following research gaps were discovered: (i) the challenges of centralised telecommunication regulatory bodies among developing countries, (ii) telecommunication fraud prevention policies and implementation challenges and (iii) challenges of telecommunication security education as a fraud prevention policy.

1.3 The Purpose of Study

The study assessed the current challenges in implementing fraud prevention telecom policies in developing countries using Ghana as a case study. It offered an independent view of the challenges and proposed alternative approaches in the form of recommendations. These recommendations are to be used to overcome these challenges to be able to regulate telecommunications services so as to minimise opportunities for the commission of fraud.

The study focused on telecommunication fraud prevention policies, implementation challenges of the fraud mitigating policies of the regulatory bodies and telecom companies vis-a-vis current trend of fraud in Ghana. This was done to gain an in-depth understanding of the frauds and to offer an independent view of the telecommunication fraud prevention policies and implementation challenges of the policies and make recommendations. Given the need for an in-depth understanding of the frauds and the challenges of regulators, the research required an interpretive philosophy or epistemological foundation [80] even though the research is exploratory in nature.

1.4 Research Question

Inferring from literature, noting the research gaps identified, one wonders whether previous challenges to the implementation of fraud prevention telecom policies were overcome or they persist? Are there new forms of challenges? How are these challenges impacting on the level of telecom fraud?

Again, knowing that these challenges vary based on geographic settings or level of development of a country and given the difficulty in conducting a holistic research that covers all geographic settings, there is a need for an exploratory single case research. This informed the choice of the research question: What are the current challenges in implementing telecommunication fraud prevention policies in developing countries?

The findings of this research provided information on whether previous challenges to the implementation of telecommunication fraud prevention policies still persist and also, revealed new challenges. The current challenges in implementing telecommunication fraud prevention polices were placed into three (3) categories namely: (a) regulators challenges, (b) operators challenges and (c) Subscribers/users challenges. Alternative approaches to overcome these challenges are provided in the form of recommendations. These recommendations and contributions are stated under the discussion section of the research document.

2 Background of existing frauds in Ghana

Fraud is define by the Chattered Institute of Public Finance and Accountancy (CIPFA) as "any intentional false representation, including failure to declare information or abuse of position that is carried out to make gain, cause loss or expose another to the risk of loss" [20]. Further, "fraud is dishonestly obtaining a benefit, or causing a loss, by deception or other means" [21]. Fraud is broadly categorize into two namely: (i) **Internal fraud,** this occurs when fraud committed against an entity is committed by its officials or contractors and (ii) **External fraud,** occurs when committed fraud comes from outside the entity from external parties such as clients, service providers, other members of the public or organised criminal groups [21].

2.1 Types of frauds

Fraudulent activities aided by information technology occur in every aspects of our daily activities and these include:

2.1.1 Identity fraud

This occurs when an individual's personal information is used by someone else without their knowledge to obtain credit, goods or other services fraudulently [20]. This process is achieved after the fraudster had employed social engineering and other means such as spoofing and sniffing victims' credentials or attacking victims via Man-in-the Middle aattack.

2.1.2 Pyramid schemes fraud (also known as chain letter scams).

The fraud scheme is usually advertised through mailings, newspapers and internet or via word of mouth [20]. The victims are asked to pay some specified amount of money to become members of a scheme which promises large commission earnings if they recruit others to the scheme [20]. If enough new members join, the pyramid grows, enabling some members to make money. Inevitably, the money runs out, and those at the bottom of the pyramid scheme lose their investment [20]. This fraud is gradually gaining grounds in Ghana and some African countries.

2.1.3 Mass marketing fraud

Employing social engineering tactics, this type of fraud is wide ranging and captures a number of different types of frauds (example, it occurs via internet, telemarketing and mails or at mass meetings) [20]. Fraudsters often seek to defraud multiple individuals to maximise their criminal revenues [20]. To do this, victims are persuaded to transfer money to the criminals in advance on the basis of promised goods, services or benefits that will follow [20]. Taking advantage of victims delayed in recognising fraudulent solicitations, fraudsters use generic, well- known fraud templates by simply recycling and updating schemes that have proven successful in the past against their victims [20].

2.1.4 Telecommunications fraud

This involves the theft of services or deliberate abuse of voice and data networks [20]. **Telephone banking fraud**, through social engineering, customers are tricked into disclosing security details through cold calling or fake emails which criminals' then use to commit fraud [20]. Details of telecommunication frauds are found in the literature review section of this thesis.

2.2 Fraud prevention

Fraud prevention involves formulating and putting in place effective accounting, operational controls and fostering an ethical culture that encourages all to play their part in protecting public resources [21]. Establishing an ethical culture is an important step in preventing and detecting fraud [21]. Telecommunication fraud prevention policy is a document that outlines the protections that should be enacted to ensure that the governments, companies/operators, organisations assets face minimal risks [17]. A security policy is a strategy for how an institution or a company will implement Information Security principles and technologies [18].

One of the security concerns of telecommunication system is the cost of having to replace all the legacy equipment which were designed without adequate security features to meet modern security threats [22]. The wealthy economies have to a large extent been able to replace some of these equipment with modern ones having advanced security features. However, this is not the case for many developing countries.

Aside the replacement of the legacy equipment, the existence of centralised regulatory authorities namely (i) the European Commission (EC) which coordinates it activities with the individual National Regulatory Authorities in member countries, (ii) the Federal Communication Commission (FCC) of the United States of America which coordinates it activities with the Public Utility Commissions (PUCs) for her individual states [23], have helped foster the design and implementation of an efficient and effective telecom policies. This enhances proper and thorough coordination between intra and inter regulatory activities as well as between both intra and inter operators [23].

This coordination serves as checks and balances, thus enhancing proper security coordination with the goal of minimising the opportunity to commit fraud. Although there exist some conflicts of interest between the individual regulators of member countries and continental blocks (EC and FCC) [23], having a centralised regulatory authority coordinating with individual national regulatory authorities has proven to be the most effective means to enhance security in the telecom industry [24], [25], [26], [27].

Despite the existence of West Africa Telecommunication Regulators Assembly (WATRA) [81] and Telecommunications Regulators' Association of Southern Africa (TRASA) [82], Sub Sahara African countries are yet to realise similar benefits achieved by the European member countries and the United States. This therefore, hinders an effective inter regulatory coordination thereby making inter border security management difficult.

In attempt to address the concerns of telecommunication, the International Telecommunication Union (ITU) [28], World Bank [29],[30], World Trade Organisation (WTO) [31], Communication Fraud Control Association (CFCA) [32], United Nations Economic Commission for Africa (UNECA) [33], the European Commission (EC) [34], West Africa Telecommunication Regulators Assembly (WATRA) [81] and Telecommunications Regulators' Association of Southern Africa (TRASA)[82], have developed and are developing telecom policies, and laws to be adopted as part of governments public policies to manage telecom operations, and also, offer advisory services to individual nations on issues of general telecommunication operations and security related issues. Individual countries have also been developing policies and laws to help curb the security concerns of telecommunication services and operations [5].

Just as various bodies, institutions, organisations and governments are making strenuous efforts aimed at addressing the security associated with telecommunication operations and services, fraudsters associated with telecommunication operations and services, are constantly spreading their areas of targets and advancing in their mode of operations so as to evade detection and apprehension [15].

The threat posed by these fraudsters means governments and operators worldwide need to always be on guard to match up to new threats and security challenges. This brings extra budgetary cost to governments and operators worldwide, and this is where the major problem of concern arises, as those with little financial resources and infrastructure turn to lag behind. This offers a partial explanation as to why there is a great disparity in terms of telecommunication system operations and services security between the advanced, wealthier economies and the developing, less wealthy ones worldwide. This makes the under developed and less wealthy economies more susceptible to telecommunication fraud.

In most literature reviewed, it appears that most of the studies done so far are focused on solutions that treat the symptoms and not the root source of the problems associated with telecommunication. This thesis reveals that the root sources of telecom fraud emanates from the fraud prevention telecom policies and how they are implemented, and also, explains why there is the need to combine telecommunication fraud prevention policies, implementation challenges, and telecom related fraud, and look at them together as they influence each other.

2.2.1 Root Source of Telecom Fraud

The security of every institution begins with security policy aimed at preventing or minimising risk [17], [18], [21]. This makes fraud prevention/security policies root sources of security to any establishment [17], [21]. Hence, anything short of the implementation of fraud prevention telecom policies resulting into fraud constitutes a root source of fraud in the telecommunication industry. Therefore, frauds in the telecom industry are either as a result of weak/ineffective policies or lack of implementation. When security policies or telecommunication fraud prevention policies are implemented, they become reference guide when matters of security arise. Security policies provide legal protection to companies and institutions [17], [21].

2.2.2 Government Telecom Policies

Most governments have a telecom policy requirement or vision of a universally available, affordable and quality telecommunication services provided through open, competitive, and well managed markets and ubiquitously adopted to the benefit of their economies and societies [5], [6], [7], [8].

2.2.3 Operators Policies

Operators formulate their policies aimed at technically implementing telecom policies set by governments and their own internal policies set to protect their business, employees as well as their assets. Occasionally, there exist conflicts of interest between operators and governments as most often their policies opposes each other’s interest at some points. This often results in compromises from both sides.

3 Summary of Literature Review

The literature review was thoroughly and systematically conducted based on the guidance approach for information system as proposed by Webster and Watson 2002 [74].

Fraud is defined as "dishonestly obtaining a benefit or causing a loss by deception or other means" [21]. Fraud is broadly categorize into two namely: (i) **Internal fraud,** this occurs when fraud committed against an entity is committed by its officials or contractors and (ii) **External fraud,** occurs when committed fraud comes from outside the entity from external parties such as clients, service providers, other members of the public or organised criminal groups [21].

Telecommunication policy (as public policy), is defined by James Anderson as a "purposive course of action or inaction undertaken by an actor or set of actors in dealing with a problem or matter of concern" [1]. Policies on telecommunication and subsequently telecommunication fraud prevention policies are part of governments' horizontal policies throughout the world.

Telecommunication fraud prevention policy is a document that outlines the protections that should be enacted to ensure that the governments, companies/operators, organisations assets face minimal risks [17]. A security policy is a strategy for how an institution or a company will implement Information Security principles and technologies [18].

"Implementation stage of the policy process is an operational phase where policy is actually translated into action with the hope of solving some public problem" [43]. According to Michael L. Best and Dhanaraj Thakur research findings, the challenges to implementing policy in the telecom industry in developing countries are; (i) weak and institutional environment, (ii) intra-governmental institutional actors and (iii) the dominance of the elite groups in decision making [2].

The advance countries are also facing a challenge in the form of conflicts of interest as to the level or extend of regulatory authorities that the centralised blocks (EC and FCC) should have on member countries and states respectively as opposed to the individual National Regulatory Authorities of member countries and states respectively [23].

In general, regulators throughout the world experience the following challenges:

(i) The telecommunication ecosystem embodies a large variety of regulations and laws, and the notion of legality significantly vary depending on the country and communication medium [22],

(ii) Lack of cooperation, law enforcement authorities have difficulties in international law enforcement which makes identification of fraudsters difficult even when the fraud is detected [22], [44]. Despite the presence of international organizations there is a lack of joint industrial initiatives to fight fraud [22] and

(iii) Most developing countries do not have legislations protecting data and hence the non-existence of official definition of identity theft [40]. In Ghana however, the parliament enacted Data Protection Act, 2012, "AN ACT to establish a Data Protection Commission, to protect the privacy of the individual and personal data by

regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters" [45].

After haven gone through several relevant literature related to fraud prevention telecom policies, its associated implementation challenges and telecom frauds resulting from either weaknesses in fraud prevention telecom policies or the lack of will to implement telecommunication fraud prevention policies, the following research gaps were identified:

(i) the challenges of centralised telecommunication regulatory bodies among developing countries,
(ii) combine fraud prevention telecom policies, implementation challenges, fraud as a consequence,
(iii) telecommunication fraud education as a fraud prevention policy.

These research gaps yet to be explored which researchers need to have a look at as we seek to enhance telecommunication/cyber fraud early detection and management so as ensure sanity in the telecommunication industry. This research however, is based on one of these yet to be researched areas and that is "fraud prevention telecom policies, implementation challenges, fraud as a consequence".

3.1 Search Procedure

The search was carried out in a rigorous and systematic manner (Webster and Watson, 2002) and was done on theme base. It was considered as a means through which literature related to the study could be better captured. In our quest to selecting literature deemed useful to the research, we employed various search engines such as ACM library, Google, Google Scholar, MIS Quarterly Library, ScienceDirect, Regulators websites and journals etc.

3.2 Literature Review

Fraud is define by the Chattered Institute of Public Finance and Accountancy (CIPFA) as "any intentional false representation, including failure to declare information or abuse of position that is carried out to make gain, cause loss or expose another to the risk of loss" [20]. Further, "fraud is dishonestly obtaining a benefit, or causing a loss, by deception or other means" [21].

3.3 Telecommunication Fraud

Communications fraud is the use of telecommunications products or services with no intention of payment [20], [32]. Frauds commonly associated with telecommunication may be listed as:

3.3.1 Telecom arbitrage fraud, Slamming and Cramming

Telecom arbitrage fraud is the exploitation of the differences in settlement rates between countries. Phone carriers often charge different interconnection rates according to the type of call or service provider involved [32]. In the CFCA 2015 survey, telecom arbitrage fraud amounted to $2.94 billion United States dollars of revenue loss.

Slamming refers to when phone carriers illegally change customers' telephone service without their permission [22], [50]. Telecom operators often fraudulently switch the local or international service provider of the customer to itself without the customer's consent and explicit notice [22], [50]. They may at times additionally charge the customer for high call

termination rates [22], [50]. Telephone service providers are obligated by law to obtain customers' permission before switching them to a different provider [50].

Cramming refers to when phone carriers illegally add charges to customers' telephone bills for services they did not authorize [22], [50]. Customers are often deceived into accepting these charges while signing promotional materials or through social engineering techniques like negative option marketing [22], [51]. Similar to slamming, telephone service providers are obligated by law to obtain customers' permission before placing charges on their telephone bill [22], [50]. Cramming and slamming are so prevalent because of customers' lack of knowledge on these scams. It is not just that customers do not take the necessary precautions to ensure that their bills are accurate, but because phone bills are confusing and difficult to understand [52].

3.3.2 Toll Free Number Fraud and Wholesale Session Initiation Protocol (SIP) Trunking Fraud

In **Toll Free Number Fraud**, the fraudster makes an agreement with an operator who allows him/her to use the operator's network to make huge volume of calls to the toll free number, this increases the bills of the toll free number owner to the operator who then in turn, shares the profit with the fraudster [22].

Wholesale Session Initiation Protocol (SIP) Trunking Fraud, this is relatively a new form of fraud but it is growing in popularity and difficult to detect [53]. With this form of fraud, the fraudster makes money by selling wholesale trunking services, using stolen credentials to terminate the call [53].

3.3.3 Wangiri Fraud and Roaming Fraud

In Japanese, "wan" means "one" and "giri" means "hang up" [22], [52]. This form of fraud, also known as "one ring and cut," targets millions of mobile phone users by making random calls from premium-rate phone lines, letting the call ring once, and then hanging up by leaving a "missed call" message on a user's phone, the scammers hope that the users will call back. When they do, this number turns out to be a premium rate number, they often find themselves listening to advertisements like subscriptions to premium chat lines or Internet services.

Roaming fraud happens when a subscriber who has used the services of a visiting network refuses to pay and either claiming ignorance, insufficient knowledge of the additional costs, or by claiming that the service was never requested. It is fraud in its most basic form, and also, it's the most common [54]. Roaming is the automatic connection to a visiting network when the user's home network is unavailable [22], [32] [50], [51], [54]. The Call Detail Record (CDR) for these roaming charges doesn't arrive to the home network until days (sometimes weeks) later, leaving a large window of opportunity for fraudulent attacks [22], [32], [50], [51],[54].

A CFCA's survey from May1, 2015 to April, 2016 revealed that roaming services was the most vulnerable to fraud. In the survey of 130 operators worldwide, Ghana was the second highest in roaming frauds after Spain. This is not a good image for a developing country like Ghana. Page 14 figure1 shows the analysis made in the CFCA's survey report [54].

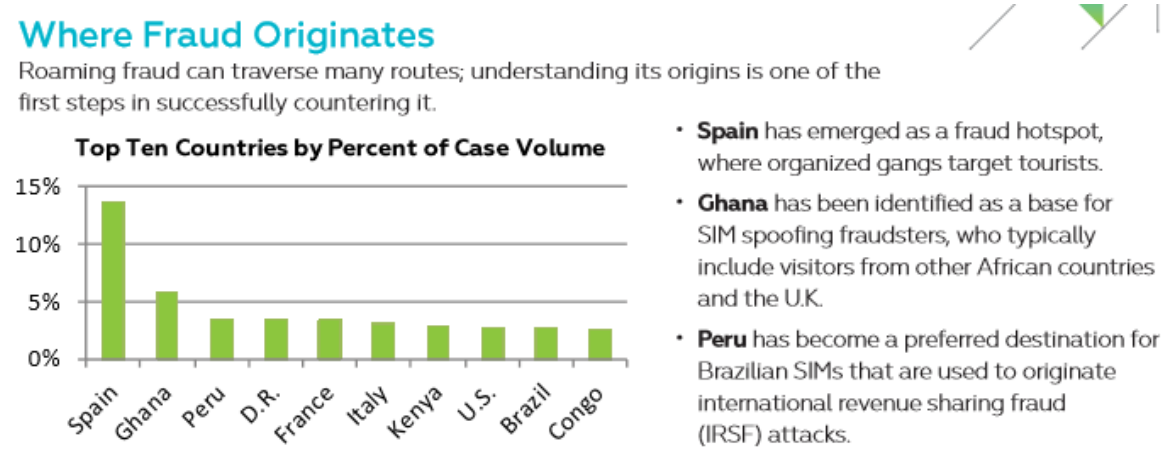

Figure 1 CFCA's May1, 2015- April, 2016 Report Analysis

3.3.4 Social Engineering

Social Engineering, this has been an old form of fraud. These fraudsters are also called Confident Tricksters. Information technology advancement has made it to grow in strength and complexity. It is the most evasive form of fraud as it is highly unpredictable and complicated as it takes so many forms which include calls, mobile text messages, emails, physical interaction and deception.

The major challenge with Social Engineering is that, it targets the users or people which constitute the weakest link to any security infrastructure. This is attested to by the famous social engineering fraudster **Kevin Mitnick** as he puts it; "I rarely had to resort to a technical attack. Companies can spend millions of dollars toward technological protections and that is wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defences or reveals the information they were seeking"[50].

It is having an unprecedented toll on developing countries' economies as they still lack the skills and knowledge to detect, control or even manage the level of spread and operations of these fraudsters. Majority of the people are completely ignorant and uneducated on these forms of fraud. Even though they experience them daily, they are left to the mercies of these fraudsters as governments and institutions either lack requisite skills, manpower or are overwhelmed. This is even further aggravated by the fact that most African countries like Ghana do not consider Information Security as a priority at both parliamentary and executive levels. Hence institutions are in a much weaker position to handle the ever advancing social engineering fraudsters.

In Ghana, social engineering has even taken a religious face [55], this is called "Sakawa" (a black magic) use to confuse, lure and even make victims fall in love with fraudsters in order for victims to send money to the fraudsters [92]. Fraudsters believe they can use it to even control the mind-set of their victims [93], [94], [95]. Their targets are mostly people from western countries, the EU countries [92], [93], [94], [101] and some affluent Ghanaians [95].

More worryingly in recent times, these fraudsters (**"SAKAWA BOYS and GIRLS"** or **"GAME BOYS"** as they preferred to be called) have taken a new turn into the telecom industry (they now engage in calls and SMS Spamming), they send fraudulent text messages and make fraudulent calls to unsuspecting mobile network subscribers. Fraudsters often take

advantage of victims delayed in recognising fraudulent solicitations and use generic, well-known fraud templates by simply recycling and updating schemes that have proven successful in the past against their victims [20]. Fraudsters' text mischievous messages to unsuspecting victims' mobile phones and luring them to either provide them their private credentials or even send money to the fraudsters accounts. This is particularly common in developing countries like Ghana.

Most often, these fraudulent messages contain information that the subscribers have won a certain promotion from the subscriber's mobile network and that the subscriber should call a certain mobile number (the fraudster's number) for more information on how to retrieve the money. When the unsuspecting subscriber calls them, they then deceive them to pay a certain amount of money into a certain bank account or mobile money account (a mobile banking system introduced into the telecommunication systems in Ghana) to be used for the processing expenses in order to forward the money to the unsuspecting subscriber. Once the money is paid, the unsuspecting subscriber never gets to hear from the fraudsters again. This strategy of the fraudsters takes advantage of the genuine promotion made by the various telecom companies in Ghana as part of their methods to reward loyal customers, promote new products and win more customers.

Another strategy often used is, the fraudster calls the unsuspecting mobile subscriber, tells the subscriber that he/she(the fraudster) is an employee of a certain company (mostly postal, telecom company, or even a reputable bank) and that they have in their possession certain items (mostly money, smart phones, ipads or laptops) meant for the unsuspecting subscriber and that the address (bank account if it is money) with which they are supposed to forward the items seems to be incomplete, as such they want the subscriber to give them the right address to effect the changes. This is a form of test to test the subscriber's intelligence and level of gullibility.

Once the subscriber goes ahead to give them his/her address without thoroughly thinking through, they know they have gotten him/her. Specifically for those fraudsters claiming to be employees of postal companies, the items meant for their victims are usually sent from the EU and Western Countries. The next stage is, they now tell the mobile subscriber that, in order to effect the changes in their "Systems" he/she will have to pay a certain amount of money into a certain bank account or mobile money account to be used as "processing fees". Again, once they get the money, the mobile subscriber never gets to hear from them again.

All contacts to the fraudster no longer works. This strategy takes into account of the gullibility and the quest for free things among Ghanaian citizens. On this same strategy, between 2005 and 2010, the fraudster used to ask unsuspecting victims to buy mobile credit and text the codes to them to be used as cost for the internet processing of their items but has since revised it to the above as subscribers were becoming aware of their exploits.

"The biggest problem is that victims of "Sakawa" and other cyber fraud activities had often not found an advertised central point in the country to report the incidences. Even when these incidences had been reported to the Ghana Police Criminal Investigation Department (CID), it has taken many years to apprehend any suspect because of the lack of know-how on tracing these criminals using computers–based investigative skills. Worse of it all, when such cybercriminals were apprehended and processed to court, there were no sufficient legal bases to prosecute these criminal as the legal system was not up to date to convict and punish cyber criminals resulting in Ghana's image being dented as a cybercrime pronged location"[57].

Romance Fraud, still on social engineering, these fraudsters exploit legitimate dating sites as well as create their own dating sites which they then use to prey on innocent women, young girls, men and young men alike who in their quest to find life time partners fall victims to these fraudsters who take advantage of their desperations and vulnerabilities to extort monies from them [93], [94], [98], [99], [100], [101]. These fraudsters, with the aid of voice pitch changing technology embedded on most phones, are able to switch their voices to either male or female voices depending on their victim's sex so as masquerade as an opposite sex to be able to convince their victims [97], [100], [101].

Skype Fraud is one of the latest fraud form targeting boys and men between ages 15-50 years who base on their positions held in an institution or society, religious or cultural settings have stronger a family relations and frowns on sexual immorality, most commonly the Islamic world and a few other geographic settings in the world [93], [94], [95], [97], [98], [99], [100], [101]. It often starts with fraudster using a beautiful young girl's picture as his profile picture on an Online Social Media platform, requesting for friendship from unsuspecting boys and young men alike [93], [94], [95], [97], [98], [99], [100], [101]. Once victims accept friendship, they are lure to have a video chat with the fraudster through Skype. On Skype, they initially chat before having a video chat.

The profile of the fraudster on the Skype still has the picture of the young beautiful girl as the picture of the fraudster. During the initial stages of the chats, the fraudster tells the victims she is feeling honey (a state of wanting to have sex or in sex mood) and wishing the victim was with her (to the victim, the fraudster is a beautiful girl who happen to fall in love with him on the online social media) so as to put the victim's state of mind in a sex mood [93], [94], [95], [97], [98], [99], [100]. The fraudster then begin describing what she is wearing , how she ready for him (the victim) despite him being far, she (the fraudster) then follows by saying the victim should turn his webcam on so they could see each other [93], [94], [95], [97], [98], [99], [100], [101].

And during this process, the fraudster then plays a video of a young girl masturbating to the unsuspecting victim while observing his state of mind and reactions. If the unsuspecting victim happens to masturbate alongside, he is recorded at the fraudster end [93], [94], [95], [96], [97], [98], [99], [100]. This is then used by the fraudster to ask for money (blackmail) from the victim and threatening of exposing the video to the family or to appropriate authorities of the country, and depending on the consequences of the exposure, the victims are made to pay huge sums of money to these fraudsters [93], [94], [95], [96], [97], [98], [99], [100]. This form of fraud has not been rampant yet in Ghana but is on the rise in other African countries.

Smishing or SMS Phishing, and Voice Phishing or Vishing (Identity Fraud); It operates similar to the normal email Phishing; its sole objective is to acquire unsuspecting subscriber's personal information such as usernames, passwords, credit card account information, and other sensitive information by posing as a legitimate company. This is done through phone calls, or even text messages [22].

Mass Marketing Fraud is wide ranging and captures a number of different types of frauds (example, it occurs via internet, telemarketing and mails or at mass meetings) [20]. Fraudsters often seek to defraud multiple individuals to maximise their criminal revenues [20]. To do this, victims are persuaded to transfer money to the criminals in advance on the basis of

promised goods, services or benefits that will follow [20]. Taking advantage of victims delayed in recognising fraudulent solicitations, fraudsters use generic, well- known fraud templates by simply recycling and updating schemes that have proven successful in the past against their victims [20].

3.3.5 Pricing Confusing, False Answer Supervision (FAS) fraud

Pricing Confusing, in this, most of the telecom operators use multiple and varying pricing plan to confuse subscribers about the real market prices of services [56]. They often provide new offers with special discounts [22], [50] and quickly change the prices once subscribers are registered [22].

False Answer Supervision (FAS) fraud, this fraud approach enable transit operators to fraudulently increase their revenue from each call by performing the following;

- **False answer or short-stopping fraud**, in this, the operator divers the call or short-stops it to a recorded message and starts charging instead of transmitting the call to the real network [22].
- **Early answer**, with this, the operator increases the call duration of the call fraudulently. This could be done by way of picking the call and playing a music or fake ringing tone until the callee actually answers [22], [58].
- **Late disconnect**, with this, the operator intentionally delay the transmission of the call disconnect message to the calling party so as to charge the caller for a longer call instead [22].

3.3.6 Interconnect Bypass Fraud or Gray Routing and Over-The-Top (OTT)

Interconnect Bypass fraud is the use of illegitimate gateway exchanges to avoid the legitimate gateways and international termination fees [22]. According to the 2015 survey of the Communication Fraud Control Association (CFCA), Simbox fraud or Bypass fraud accounted for an amount of $5.97 Billion (USD), the second highest fraud losses after International Revenue Share Fraud [32]. From the report of the United Nations Economic Commission for Africa on tracking illicit financial flow in African countries (UNECA 2015), the government of Ghana reported that SIM box fraud has cost $5.8 million in stolen taxes alone [33].

The challenge to the governments and the telecom industry is further aggravated by the emergence of a new variant of this fraud called Over-The-Top (OTT) Bypass fraud also known as Over-The-Top (OTT) Hijack fraud. OTT applications include WhatsApp, Viber, IMO, Twitter, Skype etc. OTT bypass fraud involves diverting a normal phone call over IP to a voice chat application on a smartphone without the caller's and operator's consent or knowledge [58]. This fraud occurs where "the OTT service provider partners with a transit operator to hijack regular calls (i.e calls originated from mobile or land line phone to a mobile phone) to terminate them over the OTT application" [58], [59].

In this form of fraud, OTT services use IP networks to implement services and often do so without involving the operators thus passing over operators [58]. Similar to simbox fraud, it is also attracted by the high international termination fees in some countries especially developing countries. As a result of the above, the fraudsters are able to evade the strict regulations placed on operators by various governments/countries even though they provide similar services [58], [62].

Over-The-Top services pose a security and privacy threats to subscribers as their personal data is often shared with these OTT applications [58], [73].

Some countries however, made attempts to regulate Over-The-Top (OTT) services [46], [59], [63]. Due to the lower in cost, video services and the preference of subscribers to chat on the OTT services, it attracts a sizeable subscriber population of subscribers of operators and this in itself cost operators a lot of revenue losses as there is a decline in normal calls and sms texts [58], [60], [61]. Hence the emergence of the OTT bypass fraud has worsen the plight of operators as they stand to lose more revenue.

3.3.7 International Revenue Share Fraud (IRSF)

International Revenue Share Fraud occurs when a fraudulent operator or a third party operator service provider advertises a range of phone numbers as International Premium Rate Numbers (IPRN) in various parts of the world, their victims whose numbers unfortunately happens to be among the range of numbers advertised are often from developing countries or small satellite operator with a high interconnect termination fee [22].The victim receives a huge telephone bill for the unauthorized calls and the fraudster collects a pay out from the company that owns the premium rate number.

From the CFCA's survey 2015, IRSF fraud was the largest loss incurred constituting an amount of $10.76 billion United States dollars of revenue [32]. The 2015 Global annual fraud loss survey report of the Communications Fraud Control Association (CFCA) indicates a decline in Telecommunication fraud losses. The survey found fraud losses to have declined 18%, monetary equivalence of $38.1 billion from 2013 [32].
In percent of global telecom revenues, fraud losses declined from approximately 1.69% to 0.40%, a decrease from 2013 [32]. The main reason for the decrease is attributed to an increase in collaboration and coordination among carriers in identifying and stopping fraudulent activity following the Communication Fraud Control Association's survey in 2013 [32].

The conclusion drawn from the 2015 CFCA's Survey is that telecommunication fraud still remains very lucrative. Though the decline in percentage telecom fraud losses in revenues globally is positive, the actual monetary value is still very huge and has had a very negative impact on telecommunication companies, businesses, governments and individuals worldwide [32].

3.4 Telecom Policy

According to Merilee S. Grindle and Thomas J.W, four contextual factors influence the development of policy in developing countries [2], [42]. These include:

(i) the level of technical analysis used in addressing the problem,
(ii) political stability and support related to the policy,
(iii) bureaucratic motivation and capacity for formulating and implementing the policy, and
(iv) international aid and support.

Furthermore, culture, literacy levels of citizens, and economic strength are some of the major factors influencing policy development in developing countries. Policies developed with no contributions from the general populace of a country might fail. And for the general populace to be able to contribute, they need to be enlightened. The contribution of the citizens will

factor in the culture of the people and cost. This often leads to compromises and neglects of the general populace contributions, hence, weak policy formulation.

3.5 Telecommunication Policy Implementation Challenges

"Implementation stage of the policy process is an operational phase where policy is actually translated into action with the hope of solving some public problem" [43]. According to Michael L. Best and Dhanaraj Thakur research findings, the challenges to implementing policy in the telecom industry in developing countries are:

(i) weak and institutional environment,
(ii) intra-governmental institutional actors,
(iii) the dominance of the elite groups in decision making [2] and
(iv) the limited understanding of policy process in developing countries is also a concern.

Many of the existing frameworks were developed using evidence from the United States of America and to a lesser extent Western Europe [2]. According to the findings of Martha Kanene Onyeajuwa, some of the challenges affecting telecom policy implementation and or enforcement in Nigeria (developing countries) are:

(i) weak institutional structures, and as a result, regulators and mobile service providers do not hold ordinary consumers interest at levels consistent with policy and law,
(ii) there are no special intervention to make basic mobile services accessible and affordable to low-income ordinary consumers and
(iii) there is laxity in enforcing rules by regulators and as a result, there is consistent and deliberate exploitation of unprotected and unsuspecting subscribers by telecom service providers [14].

After going through several literature relating to fraud prevention telecom policies, implementation challenges, and telecom fraud, we decided to categorize them into formal controls challenges as regulators challenges, technical control challenges as operators' challenges and informal control challenges as subscribers' challenges so as to make clearer what has been discovered by fellow researchers globally.

3.5.1 Regulators Challenges

Regulators worldwide face variety of challenges influenced by factors such culture, geographic settings, level of technology, economic strength, literacy rate of citizens, etc. The most common challenges are listed as follow:

- The telecommunication ecosystem embodies a large variety of regulations and laws, and the notion of legality significantly vary depending on the country and communication medium [22].
- Lack of cooperation, law enforcement authorities have difficulties in international law enforcement which makes identification of fraudsters difficult even when the fraud is detected [22], [44]. Despite the presence of international organizations there is a lack of joint industrial initiatives to fight fraud [22].
- There exist a conflict of interest as to the level of responsibilities of regulation between the centralised blocks, the European Commission (EC) and the individual National Regulatory Authorities (NRAs) for EU and the Federal Communication

Commission and the Public Utility Commissions (PUCs) of the individual states of the United States of America [23].

- "Two problems arise in relation to the prosecution of telecommunications offences which have an international aspect: first, the determination of where the offence occurred in order to decide which jurisdiction's law to apply and, secondly, obtaining evidence and ensuring that the offender can be located and tried before a court. Both these questions raise complex legal problems of jurisdiction and extradition. Even if one is able to decide which law is applicable, further difficulties may arise in applying that law. Extraterritorial law enforcement costs are often prohibitive."[16]
- Most developing countries do not have legislations protecting data and hence the non-existence of official definition of identity theft [40]. In Ghana however, the parliament enacted Data Protection Act, 2012, "AN ACT to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters" [45].

3.5.2 General Challenges of Telecommunication network Operations

The telecommunication infrastructure worldwide experience common fundamental challenges of which the advanced or developed countries have made tremendous efforts to overcome some but this is not same for the under developed or developing countries due to difference in levels of technology, economic strength and other factors.

Below however, is a list of some of the technical challenges telecom operators' worldwide experience:

- Over-The-Top services (OTT) which work on top of data links are mostly/generally out of operators' control [22], [46], [47], [48].
- Unlike in IP networks, the routing of a call is very often opaque. Each operator knows only the next hop of the upstream and downstream routes as well as the originating and destination number [22].
- Due to privacy issues and competition, operators usually are not willing to share or publish their pricing terms, routing options or fraud related findings [15], [16], [22], [49].
- Operators often do not have the same incentive levels to fight fraud [22].
- Roaming CDRs are not immediately available to the home operator, this makes detection and stopping of fraud difficult to the home operator [22].
- Lack of due diligence partnership agreements make call traffic vulnerable to fraud if one party has fraudulent intentions (The process of checking the quality and reliability of a transit operator before the partnership agreement is called due diligence [22]).
- The cost of upgrading the legacy systems. The legacy systems that lie in the core of telephony network were not designed with security in mind. Upgrading these legacy system worldwide is not feasible in near future due to the high cost [22]

3.5.3 User/Subscriber Challenges

Subscribers worldwide experience the following challenges:

- Lack of security awareness makes users/subscribers prone to manipulations by fraudsters [22].

- Negligence or naivety, carelessness of users of subscribers constitute a fertile ground for exploitation by fraudsters [22].
- There is generally low confidence in the legal protection of personal privacy [40].

During the formulation of a security policy, critical assets, services and values of institutions, companies and organisations are identified and the security policy formulated aimed at providing maximum protections as much as possible. However, institutions, companies and organisations grow constantly in terms of assets, services and values. These constant changes in terms of growth, demand re-adjustments in security policies techniques and technical know-how. This increases extra budgetary cost of institutions, companies and organisations. Depending on the economic strength and expertise of the institution, company or organisation, various options are often employed, some of these include;

(i) willing to compromise security for functions/services,
(ii) upgrading security policies, structures and equipments, etc.

The level of expertise and technical know-how of an institution, company or organisation determines the depth, effectiveness and efficiency of a fraud prevention security policy formulated. It is only after implementing security policies that it becomes a reference guide when matters of security arise.

Fraud occurs when a weakness in a security policy and structure is discovered and exploited by fraudsters either for personal gains or fun. Most times, it is not just about weakness in the fraud prevention security policy and structure, but the lack of effective and efficient implementations of well-defined fraud prevention security policies. This may be attributed to so many factors stated above or in the findings in this research below. There are so many frauds in the telecommunication industry associated with the exploitation of weaknesses in fraud prevention security policies and structure or the lack of effective implementations of the fraud prevention security policies as stated in the beginning of the literature review (this section).

After haven gone through several relevant literature related to telecommunication fraud prevention policies, its associated implementation challenges and telecommunication frauds resulting from either weaknesses in telecommunication fraud prevention policies or the lack of will to implement telecommunication fraud prevention policies, the following research gaps were discovered: (i) the challenges of centralised telecommunication regulatory bodies among developing countries, (ii) telecommunication fraud prevention policies and implementation challenges and (iii) challenges of telecommunication security education as a fraud prevention policy. These researchers need to have a look at as we seek to enhance telecom/cyber fraud early detection and management so as ensure sanity in the telecommunication industry. This research however, is based on one of these research gaps and that is “telecommunication fraud prevention policies, implementation challenges, fraud as a consequence”.

4 Research Methodology

Given the nature of the research as real life phenomenon as put by Yin and Darke, case study as an empirical inquiry that investigates a contemporary phenomenon in real life [75],[76] and since the research requires engaging in the phenomenon, field study was seen as most appropriate [77],[78],[79], [80].

Field research method was used to collect data from the various institutions involve in telecom policy design, telecom policy implementation and telecom policy enforcement regarding the provision of telecommunication services and operations in Ghana.

4.1 Research Setting

The setting of the research is in Ghana, West Africa. Ghana is located on the Gulf of Guinea, only a few degrees north of the Equator. The climate of Ghana is tropical, the eastern coastal belt is warm and comparatively dry, the south-west corner of Ghana is hot and humid, and the north of Ghana is hot and dry.

Ghana is one of the first countries in Africa to liberalise and deregulate its telecommunications sector. Ever since the privatisation of Ghana Telecom (the state own telecommunication company) in 1996 there has been a rapid growth in market competition across the mobile and internet sectors, with a number of new players being licensed to offer services.

A developing country with multiple ethnic groups and with different languages, low economic strength, low level of education and security awareness of subscribers, and low level of technology. Ghana's features and cultural settings mimics most developing countries especially those in sub-Sahara African countries. This aids in generalisation to countries with similar characteristics. The research is qualitative and exploratory in nature. The topic of the research is more of behavioural analysis or determination so qualitative method is feasible.

4.2 Motivation

The reason for using field study method is to have first-hand information, make observation and create a cordial relationship with participants or interviewees so as to create room for accessibility. This is very necessary due to sensitivity of the area of research. Without the physical knowledge and some little degree of trust of the researcher by regulators, it is highly unlikely to get any data from the regulators due to security sensitive nature of area and topic of research.

4.2.1 Reliability of Research Method

Due to the nature of the work of participants, their availability for interviews was difficult. To overcome that, there was the needed to be ready whenever participants were available to be able to perform interviews. A structure questionnaire was used as an alternative instrument for participants who never really had time to sit for interviews.

Further, participants were given the option to schedule their own time for the interviews so as to make them more comfortable and willing to participate. Interview questions and the questionnaires were open-ended to make participants contribute and also to avoid being bias, very polite, simple and straight forward to avoid intimidation and ambiguity. Again, we

ensured that the anonymity of participants was guaranteed in both interviews and questionnaires due to the sensitivity of the research area.

Given the numerous advantages associated with field study, it was the best option to use Field Research method to help collect data from the various institutions involve in telecom policy design, telecom policy implementation and telecom policy enforcement regarding the provision of telecommunication services and operations in Ghana.

To complement and consolidate data, literature relating to telecommunication fraud, telecommunication fraud prevention policy and its associated implementation challenges were also reviewed. Government Journals, Regulators Websites, Video Recordings of interviews of fraudsters were also used.

4.2.2 Validity of Research Design-Method and Procedures

In using field study research method, it was possible to have access to the inner circles of regulators and access to participants for interviews. Given the access privilege gotten, it was possible to schedule interviews and also make observations.

Primary data on telecom policies and subsequently telecommunication fraud prevention policies were collected from the Ministry of Communication and the various telecom regulators in Ghana. This was done via interviews and the use structured questionnaire to obtain data on telecommunication fraud prevention policies implementation challenges from the managers and people in charge on telecom security at the Ministry of Communications and at regulatory authorities.

Interview questions and questionnaire were open-ended to avoid personal biasness. An excerpt of the questionnaire can be found in the appendix of this research document. The questions were polite, straight forward and unambiguous and brief. Filters were also used in questionnaire to help respondents skip questions not applicable based on a response given to a question prior to the next question.

Publicly available documents at regulators websites [5], [19], [21], [38], [39], [41], [64], [67], [68], [70] and pre-recorded video recordings of interviews conducted by various journalist with telecom/cyber criminals both inside and outside Ghanaian prisons were used as secondary data. The video recordings were used to learn their modus operandi and also, to serve as evidence [92], [93], [94], [95], [96], [97], [98], [99], [100], [101]. The video recordings were conducted between years 2010-2018 at different stages by different journalist. Some of the videos are experiences of victims [96], [101]. Only a few of the recordings are in English language [92], [100], [101]. The rest are in the local Ghanaian language.

Further, relevant literature relating to telecommunication fraud prevention policies, implementation challenges and telecommunication related frauds were also used to augment findings.

Analysis of data was done using logic model proposed by Robert K. Yin [75] base on content analysis as proposed by Klaus krippendorff [102].

4.2.3 Research Procedures

Though the research is an exploratory case study as proposed by Robert K. Yin [75], the requirement of an in-depth understanding of the frauds and challenges of the regulators makes the research to have an interpretive philosophy or epistemological foundation as stated by Gonzalez, Dahanayake [77], Chen and Hirschheim [78], Klein and Myers [79] and Mitev [80].

Primary data on telecom policies (fraud prevention telecom policies) were collected from the Ministry of communication and the various telecom regulators in Ghana. We also used questionnaire to obtain data on policy challenges from the managers and people in charge of telecom security at the Ministry and regulators offices.

Open-ended interview questions and questionnaire were used to collect primary data from the Ministry of Communication, National Communication authority (NCA), Afriwave Telecom limited, Bank of Ghana, Operators and Ghana Police Service. The rationale for using open-ended questionnaire as against close-ended questionnaire was to reduce personal biasness and to allow participants to willingly and freely give their responses without restrictions since the research is exploratory in nature. Again, to ensure the anonymity of participants were guaranteed in both interviews and questionnaire due to the sensitivity of the research participants personal details were not required.

The participants were policy makers and security personal in charge of telecom fraud prevention and management. Both interview questions and questionnaires were polite, straightforward, simple in wording and unambiguous. Filters were also used in questionnaire to help participants respond quickly. The questions were very brief in terms of length and number. A copy of the questionnaire can be found in the appendix. Page 24 table1 is an excerpt of what was done.

Institution	Research Instruments used	Number of participants	Number of respondents interviewed	Number of questionnaire sent	Number received
Ministry of Communication	Interview/ questionnaire	1	1	1	1
National Comm. Authority	Interview/ questionnaire	3	3	1	1
Afriwave Ghana ltd	Questionnaire	1	0	1	1
Bank of Ghana	Interview/ questionnaire	3	3	1	1
Ghana Police Service	Questionnaire	1	0	1	1
Operators	Questionnaire/ interview	1(MTN)	1	6	1
National Information Tec. Agency	Questionnaire	1	0	1	0
Total		11	8	12	6

Table 1 Institutions and instrument used to collect data

4.3 Data Collection

We collected data on the current telecom policy, telecom policy implementation challenges and also intended to obtain data on the corresponding economic and security impact on telecom fraud in the country Ghana for the past five (5) years from the various telecom regulatory institutions (NCA, AFRIWAVE Telecom Limited, NITA, Bank of Ghana) and the Ministry of Communication, the rate of telecom fraud for the same period from the Ghana Police Service, but were unable to get the statistics either due to the nonexistence of such statistics in the case of the Ghana Police Service because of the fact that the Police Cyber Unit was just established in 2016 or the unwillingness to provide recorded statistics on the part of the NCA, Ministry of Communication and operators.

Publicly available documents at regulators websites and pre-recorded video recordings of interviews conducted by various journalist with telecom/cyber criminals both inside and outside Ghanaian prisons were used as secondary data. The video recordings were used to learn their modus operandi, augment the data obtained and also, to serve as evidence. The video recordings were conducted between years 2010-2018 at different stages by different journalist. Some of the videos are based on the experiences of victims. The data collected were stored in a field note book, a pendrive (both recorded video and soft copy of participants' response) as indicated in the page 25 table 2.

Data source	Role	Data collected
Ministry of Communication	Political/executive arm of government and policy formulator	Role, telecom policy including fraud prevention telecom policy, challenges
Bank of Ghana	Policy formulator	Mobile banking policy, challenges
National Comm. Authority	Regulator	Role, fraud prevention telecom policy implementation challenges
Afriwave Ghana ltd	Regulator	Role, challenges
National Information Tec. Agency	Regulator	Role
Operators	Technical/operationalise implementers	Challenges
Ghana Police Service	Law enforcer	Role, challenges
YouTube (interview recordings of fraudsters)	Telecom/cyber criminals	Exploits, motivation, strategies

Table 2 Data source and type of data collected

4.4 Data Analysis

The analytic technique used to analyse data is logic model as proposed by Robert K. Yin [75] based on content analysis as proposed by Klaus krippendorff [102], was performed on both primary and secondary data collected with unit of analysis being Ghana. Below are excerpts of the analysis:

4.4.1 Coding

Table 3 is the analysis of data gotten from participants.

Primary challenges	Sub challenges related to primary challenge
Education	Security awareness
Laws and regulations	Lack of cooperation, lack of coordination, many implementation agencies, Conflict of interest, jurisdiction and extradition laws, bureaucratic procedure.
Economy	Economic strength, Quest to earn high revenue in termination, sustain economy and telecom operation
Fraud	Obtaining evidence, Concealment of information, losing customers, negligence, naivety, carelessness
Technology	Infrastructure deficit
Politics	Corruption, laxity

Table 3 Content analysis of received data

The analysis on the data obtained from participants indicates that education of subscribers on telecom and cybersecurity has not been so effective leading to poor security culture and very low level of security awareness among subscribers. This increases naivety, negligence and carelessness among subscribers. And this renders most of the technical security features implemented ineffective as subscribers provide a fertile ground for attacks.

Laws and regulations, different telecom laws and regulations practice by different developing and lack of proper cooperation and coordination between inter regulatory bodies of members of developing countries constitute a big challenge in tackling inter border related telecom or cyber frauds. This lack of coordination and cooperation between inter regulatory bodies of members is a major setback in managing and curbing telecom and cyber frauds as jurisdiction and extradition laws hinder the apprehension of criminals.

Again, the existence of so many implementation agencies with lots of bureaucratic procedures and lack well defined roles makes it difficult and confusing in the handling of matters relating to telecom or cybercrimes in Ghana.

Economy, Ghana's weak economic strength makes it difficult to rely on her scare resources to sustain the economy, telecommunication operation and services without depending on

revenue generated from the high international calls termination fees. Fraudsters take undue advantage of this to engage in Sim Box and Over-The-Top bypass frauds.

Frauds, obtaining evidence of criminals from operators of different developing countries and operators within Ghana to tackle telecom fraud is very challenging as operators are often concealing evidence to avoid losing customers. The lack of proper coordination and cooperation between inter regulatory bodies of members of developing countries freezes out efforts to trace frauds and fraudsters.

Technology, the telecom infrastructure in Ghana, as in most developing countries throughout world, is still mostly legacy equipment and not up to date with modern advance security features to tackle fraud as found in the advance world. Hence technically weak to defend advance technical attacks. Aside the infrastructure deficiencies, there is also low level technical expects to handle and manage telecom frauds.

Politics, Ghanaian government is trying avoid over militarization of the telecommunication sector as it seeks to liberalise the sector to encourage growth and expansion of the sector constitute its weakness as the telecommunication operators take advantage of the lenience in restriction to exploit subscribers and government. This partially account for why there is the laxity in implementing telecommunication fraud prevention policies.

4.4.2 General Trend of Fraud in Ghana for the year 2016

The challenges encounter in implementing telecommunication fraud prevention policies or due to inefficiencies in the telecommunication fraud prevention policies as depicted in the coding has negatively impacted telecommunication services security in Ghana. Telecommunication and cyber related fraud trend is currently high Ghana. Page 27 figure 2 indicates analysis of reported cybercrime cases for year 2016 to the Criminal Investigation Department of the Ghana Police Headquarters.

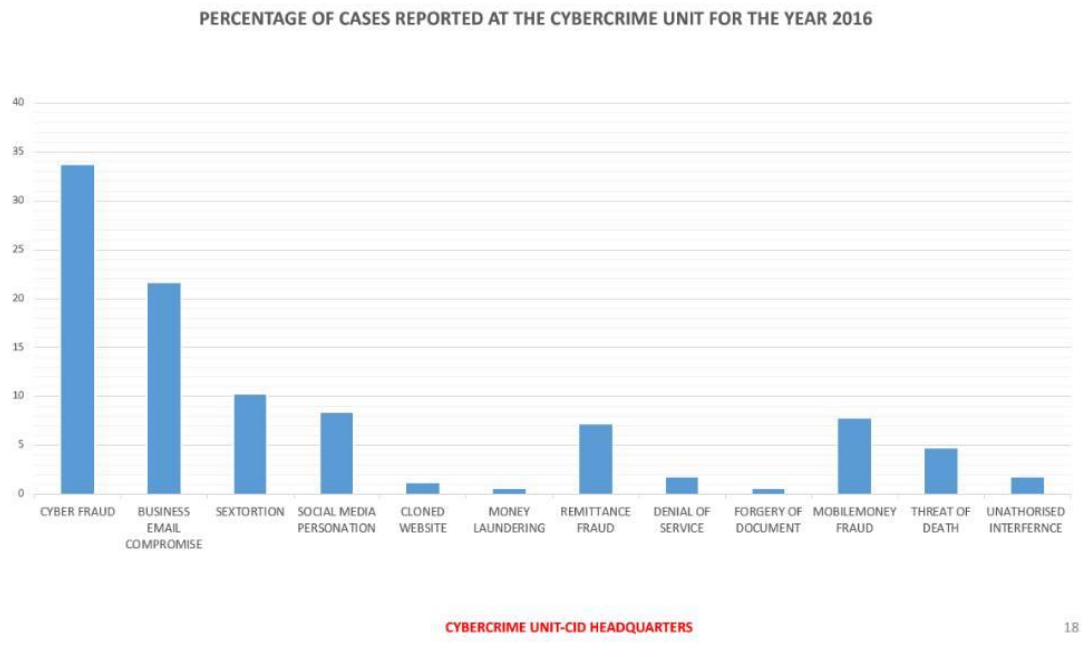

Figure 2 Ghana Police Service CID Cybercrime Unit Analysis report for 2016.

The Ghana Police Cyber unit was established in 2016 and as result, they were not able to provide me with data for years before 2016. Again, the police was unable to provide me with real figures (data) for me to do my own analysis due to the laws restricting them to give out figures (data).

A total of 397 cases were reported to the cybercrime unit of the CID of the Ghana national police service for 2016. Inferring from figure 3, it is very clear that **Cybercrime** (cyber fraud, business email compromise, **social engineering** (Sextortion, Mobile money fraud, Remittance fraud, Social media personification), Cloned website, Denial of service) rate is very high. The chart only represents less than twenty percent (20%) of the reported Cybercrimes committed, the remaining over eighty percent (80%) is unaccounted for because the victims have not reported or probably did not report to the appropriate authorities as a result of ignorance and lack of education. The rate however, is expected to rise as against the ill-equipped police service.

5 Results/findings

To establish a relationship between the coding analysis of participants' response and analysis of the data provided by the Ghana Police Criminal Investigation Department (CID) Cybercrime Unit, it is necessary to examine the roles the various institutions responsible for telecommunication and cyber related security in Ghana whose challenges are negatively impacting telecommunication operations, security and cybersecurity.

After examining the roles of these institutions responsible for telecommunication operations, security and cybersecurity, their challenges are then clustered into: (a) regulators challenges, (b) operators challenges and then (c) subscribers/users challenges. The clustering is done to give a picture of the relationship between the roles of the institutions, the challenges they face and how the challenges impact on telecommunication operations, security and cybersecurity in Ghana. The relationship established is then use to compare with previous research findings in the discussion. The following finding were obtained:

5.1 The Roles of the Various Regulatory Institutions in Ghana in Relation to Telecommunication

Below is a list of the various policy developers, implementers and their assigned roles in managing telecom operations and services in the Republic of Ghana. The choice of developers and implementers is motivated by their responsibility in the general security as well as specific security roles play by providing security in Ghana as a whole, and telecommunication operations and security, and cybersecurity as a specific area related security in Ghana.

5.1.1 The Ministry of Communication

The Ministry Communication is the executive arm of government responsible for communications and its related areas (telecommunication, ICT, etc) [64], "The Ministry of Communications (MoC) has the core responsibility of initiating and developing national policies aimed at achieving cost effective information and communications infrastructure and services, for the enhancement and promotion of economic competitiveness in line with the policy guidelines of the Medium Term National Development Policy Framework (MTNDPF) developed as the basis of Ghana Shared Growth and Development Agenda (GSGDA) II 2014-2017"[64]. Below are the objectives of the Ministry of Communication of the Republic of Ghana;

- "Initiate and formulate ICT policies taken into account the needs and aspirations of the people.
- Coordinate, monitor and evaluate the efficiency and effectiveness of the performance of the Communications Sector.
- Develop appropriate regulations to protect consumers and stimulate competition in the communication sector.
- Build capacity for the ICT sector"

Aside the above, it again drafted the National Cyber Security Policy and Strategy in March 2014 [57], in attempt to ward off cyber criminals and also to prepare the nation in the event of cyber-attack. This is seeking to create awareness and ensure capacity building among citizens to be able to prevent and possibly handle cyber-attacks in the event they occur.

5.1.2 The National Communication Authority (NCA)

National Communications Authority Act, 2008, established the National Communications Authority as the central body to license and regulate communications activities, services in the country and to provide for related purposes. It was established by Act 769 of the Parliament of the Republic of Ghana on 11th December, 2008 [65]. The NCA is the main implementation agency established by law by parliament of Ghana to handle communication and its related issues. Below are the roles of the NCA [66]:

I. "**Grant licenses and authorisations for operation of communication systems and services**

NCA assigns, allocates and regulates the use of frequencies in conformity and development strategies for the communications industry. NCA is responsible for managing civilian access to radio spectrum. Their work involves releasing spectrum for new uses, as well as developing policies such as spectrum trading and spectrum pricing to ensure that spectrum is used efficiently. They also monitor the airwaves 24 hours a day to identify cases of interference, take action against illegal broadcasters and users of unauthorised wireless devices.

II. **Ensure fair competition among licensees**

The core responsibility of NCA is to promote and ensure fair competition in the telecommunications industry. These include implementing policy on competition within the remit of the Authority. NCA promotes fair competition and protects communications services providers from misuse of market power or anti-competitive and unfair practices by other service providers. The Authority is also vested with concurrent powers to deal with anti-competitive behaviour in broadcasting, use of spectrum and telecommunications.

III. **Establish and monitor quality of service indicators for operators and service providers**

The Authority continuously strives to ensure that consumers get good quality from any telecommunications services, be it voice or data. The Authority routinely conducts network end-to-end quality of service monitoring exercises throughout the nation. This exercise is done once every quarter in all Metropolis in Ghana and twice a year in all the Municipal and Districts in the country. The result of qualities of service surveys are used for compliance and enforcement purposes, thereby ensuring that consumers are provided with excellent service throughout Ghana.

IV. **Educate and Protect Consumers**

The Authority ensures consumers are protected by providing safeguard mechanisms for seeking redress on telecom issues. Acting as a neutral arbitrator, NCA examines and resolves complaints and disputes between subscribers, licensed operators or any other person involved in the communications industry.

V. **Authorise Type Approval and and Enforce Equipment Standards**

Equipment standards and type approvals are administrative but technical requirement for vendors, manufactures, dealers and network service providers to proof that their communications equipment that are sold, used and meant to be connected to the public networks have met the required national and international standards. It is aimed at ensuring that communication equipment that come and are used in the country has met the required standards, are safe, secured and does not cause any interference to public networks ,a basic requirement to ensure end to end network quality of service delivery.

VI. **Coordinate International Frequency**

To ensure good quality of service for consumers, the Authority constantly engages in international frequency coordination with our neighbouring countries particularly Burkina Faso, Cote D'Ivoire and Togo. This is to ensure that telecommunications services and broadcasting services provided in our country are not interfered with by other transmitting signals from these countries".

5.1.3 The National Information Technology Agency (NITA)

"The National Information Technology Agency is a public service institution established by Act 771 in 2008 as the ICT policy implementing arm of the Ministry of Communications. NITA is the agency responsible for implementing Ghana's IT policies. Its mandate includes identifying, promoting and developing innovative technologies, standards, guidelines and practices among government agencies and local governments, as well as ensuring the sustainable growth of ICT via research and development planning and technology acquisition strategies to facilitate Ghana's prospect of becoming a technology-driven, knowledge-and values-based economy as espoused in the e-Ghana project which ideally seeks to assist the Government generate growth and employment, by leveraging ICT and public-private partnerships[67].The establishment of the National Information Technology Agency is essential for e-Government to take off in Ghana. E-Government, being an essential component of the e-Ghana project will contribute to improved efficiency, transparency and accountability in selected Government functions" [67].

5.1.4 Afriwave Telecom Ghana Limited

The license issued to Afriwave Telecom Ghana limited by the National Communications Authority, is to enable it to provide the following services [68]:

I. This Licence shall be for the provision and operation of Clearinghouse services using radio, cable, satellite or a combination of any of these systems deployed for the purpose of providing point-to-point or point-to-multipoint communication for the connection to Service Providers for the conveyance of voice, data and video.
II. The capability to connect and route voice, SMS, MMS, or any other telecommunications traffic between Service Providers and to monitor traffic volumes of each Service Provider.
III. Facilitation of monthly reconciliation among connected Service Providers among other Financial Clearinghouse services.
IV. Operating and maintaining Anti-fraud Management systems for Service Providers and Government.

V. The capability to authenticate mobile number registrations before any service activation.
VI. The provision of Equipment Identity Registry (EIR) services and ensure only type approved equipment are activated for use for any Service.
VII. Provision of data packet measurement and differentiation tools for Quality of Service and Price Regulatory compliance.
VIII. Connectivity to Number Portability Services, Bank Switch, and Internet Connect Exchange respectively as and when required.
IX. The capability, if needed, to host local and international Over-The-Top (OTT) service providers.
X. The capability to provide a common infrastructure for Government Agencies to host ICT Systems and Applications and to store confidential data securely.

5.1.5 The Ghana Police Service

The Ghana Police service is an implementation and enforcement arm/agent of the government of Ghana. It was established during the colonial days and subsequently legally backed by an act of the parliament of Ghana, Act, 1970 (Act 350) [69]. The main functions from include [70]:

- Prevention and detection of crime,
- Apprehension and prosecution of offenders,
- Maintenance of law and order,
- Protection of life and property.

With the introduction of Information Technology and being a member of the global INTERPOL, the following functions are added;

- Operational and investigative support
- Cyber intelligence and analysis
- Digital forensics
- Innovation and research
- Capacity building

INTERPOL partners with any law enforcement agency looking to investigate crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local law enforcement with focused cyber intelligence, derived from combining inputs on a global scale [71].

5.2 Telecom Fraud Prevention Policy Implementation Challenges in Ghana

The research found the found the following as some of the challenges encounter in implementing telecommunication fraud prevention policies in Ghana which have been categorised as:

5.2.1 Regulators Challenges Pertaining to Ghana

The data obtained from regulators revealed that, regulators in Ghana experience the following challenges in addition to the common challenges experienced by regulators globally as stated in the literature review section:

I. Inefficient telecommunication fraud prevention policies. The telecommunication fraud prevention policies are outdated and seem to be formulated reactively (lack users/subscribers input and enforcement as required of information security framework for designing and formulating security policies as the people in charge of designing and formulating security policies are often not necessarily technical experts but political party favourites or appointees), lack the implementation component of education and awareness creation for users or subscribers.

II. Lack of adequate legislation on telecommunication fraud or cyber fraud telecommunication operators to adhere to. There is no sufficient and up-to-date legislative laws enhancing fraud mitigation in the telecommunication industry.

III. There are too many implementation agencies which makes it difficult in identification of roles. This again creates lengthy bureaucratic procedure causing unnecessary delays.

IV. The quest to earn high revenue in the termination of international calls to sustain the economy and telecom operations in Ghana is also serving as a motivation for fraudsters to engage in Simbox fraud or Bypass fraud.

V. There is lack of proper coordination between the various implementation agencies. This hinders the ability inter operate and sharing of sensitive security information to counter fraud.

VI. Obtaining evidence of criminals from operators of different developing countries and operators within Ghana to tackle telecom fraud is very challenging as operators are often concealing evidence to avoid losing customers. The lack of proper coordination and cooperation between inter regulatory bodies of members of developing countries freezes out efforts to trace frauds and fraudsters.

VII. Inadequate skilled human resources. There is a very low level technical experts with the technical knowhow to assist in the formulation of fraud prevention telecom policies and even with the few available technical experts consideration is giving to only political party sympathisers.

VIII. Lack of financial resources to implement telecom policies. As a low income country, Ghana's financial constraints are also limiting her ability to carry out full implementation of telecommunication fraud prevention policies and other policies without soliciting international financial aids.

IX. Lack of skilled man power to fend off mobile banking (mobile money) fraudster and also, there are difficulties in ensure physical security of mobile banking (mobile money) merchants.

X. Laws and regulations, different telecom laws and regulations practice by different developing and lack of proper cooperation and coordination between inter regulatory bodies of members of developing countries constitute a big challenge in tackling inter border related telecom or cyber frauds. This lack of coordination and cooperation between inter regulatory bodies of members is a major setback in managing and curbing telecom and cyber frauds as jurisdiction and extradition laws hinder the apprehension of criminals.

XI. Lack of reporting of telecommunication fraud incidence by subscribers to appropriate authorities hinders regulators ability to estimate how wide spread the various telecommunication fraud schemes are operating in Ghana.

XII. Political influence, Ghanaian government is trying avoid over militarization of the telecommunication sector as it seeks to liberalise the sector to encourage growth and expansion of the sector. This constitute its weakness as the telecommunication operators take advantage of the lenience in restriction to exploit subscribers and government. This partly account for why there is the laxity in implementing telecommunication fraud prevention policies. Again, the political polarisation of almost every sector is negatively effecting governments' ability to tackle fraud in Ghana. Associating the various operators with the two major political parties (example MTN to the National Democratic Congress and Vodafone and Globacom to the New Patriotic Party).

XIII. Corruption, the political polarized nature of Ghana, weakens governments bid to enforce telecommunication fraud prevention policies aim at tackling telecom frauds thereby breeding corruption. This partially account for why there is the laxity in implementing telecommunication fraud prevention policies.

5.2.2 Reasons for Operators Lack of Will to Implement Policies besides Technical Reasons.

Aside the most common challenges experienced in implementing technical policies globally, operators in Ghana seems to have taken advantage of the weaknesses of regulators to exploit subscribers. The research revealed the follow;

- Most operators are reluctant to implement fraud prevention telecom policies for fear of losing customers. Operators fear that if they enforce strict security policies it makes their customers/subscribers uncomfortable using their platforms which may cause them to leave their platforms for others which they feel comfortable with.
- Lack of up-to-date infrastructure and technology to implement telecom policies. The existing infrastructure is still mostly legacy equipments and vulnerable to modern security threats.
- The many uneducated subscribers is a challenge to operators in Ghana. Getting them to under telecommunication related security is difficult.
- Lack of political will or the laxity of regulators to implement and enforce telecom policies on fraud due to fear of over militarization which may depresses mobile penetration, chasing away potential investors which inhibits the liberalization process which most governments seek to achieve. This gives operator a lop hole to exploit.

5.2.3 User/Subscriber Challenges Pertaining to Ghana

Due to the geographic setting, culture, literacy rate of the country Ghana, it was revealed that, the user/subscriber faces the following challenges:

I. Lack of education and awareness, most subscribers are uneducated and even those educated are not educated on telecom related fraud. The lack of security and awareness education from regulators and operators to subscribers makes it difficult for subscribers to adhere to the telecommunication fraud prevention security policies set out by the regulators and operators. Most subscribers are ignorant of the frauds

existing in the telecommunication sector even though they experience them daily. The security culture in Ghana and most developing countries is generally very poor.

II. Negligence, some subscribers fall victims due to negligence. The negligence exhibited by most subscribers make them prone to fraudsters who prey on them daily.

III. Poverty, poverty makes most subscribers more gullible to fraudsters who pretend to want to help them. Poverty makes most of them to easily trust fraudsters who masquerade as good people wishing to help them. This makes them to easily fall for social engineering and pyramid scheme fraud exploits.

IV. Most subscribers do not actually know which body/institution to report telecommunication frauds to. The lack of a decentralised incidence response units/offices nationwide and the reliance of the short code emergency lines makes it difficult for victims to report crimes. Illiterates do not even know of the existence of the emergency short codes left alone memorising the codes. Even some of the literates hardly remember the emergency short codes to call to report crimes. Besides, when crimes are even reported, it takes almost forever to get the desire response making victims more apprehensive and insecure.

V. Quest for free things and quick money, the desire of most subscribers to obtain things for free and to get money quick make them more prone to fraudsters.

5.3 Billing Related Fraud in Ghana

Billing related fraud appears to have been one of the most elusive form of frauds in Ghana as there is often little or no public discussions or literature in matters related to telecom related fraud.

5.3.1 Pricing Confusion

Using multiple and varying pricing plan to confuse subscribers about the real market prices of telecommunication services. Given the fact that majority of the mobile subscribers in Ghana are uneducated, and even with the educated ones, a large percentage of them are not enlightened on telecommunication related frauds. This makes it easy for the mobile operators to get away with this kind of frauds and manipulations.

The nature of this price manipulation frauds, makes it difficult for majority of subscribers to detect since most of them only care about their calls going through. The few sensitive ones who are able to detect the price manipulations, do not also know whom to report to or how to report it. The current policies and laws are not equally helping the citizenry regarding these frauds leaving the citizens at the mercies of the operators. Pricing Confusion is very common in Ghana.

5.3.2 False Answer Supervision (FAS) fraud

The fraudulent approach used by transit operators to increase their revenue from calls of unsuspecting subscribers. Details about this kind of fraud is explained in the literature review section. Similar to the price confusion, most Ghanaians often put the blame on their phones for not allowing them to terminate their calls in-time, network jam or the recipient for call being picked and not talking (responding). Had they any knowledge of this fraud, they would have known whom to put the blame on and possibly report if only they also know who to report to.

5.3.3 ByPass or Simbox Fraud

Using illegitimate gateways exchanges to avoid the legitimate gateways and international termination fees. The quest to earn high revenue in the termination of international calls to sustain the economy and telecom operations in Ghana is also serving as a motivation for fraudsters to engage in Simbox fraud or Bypass fraud. This challenge has just gotten worse for Ghana and other developing countries as a new variant of this fraud known as Over-The-Top (OTT) Bypass fraud just emerged.

6 Discussion

The research found the current challenges in implementing fraud prevention telecom policies in developing countries using Ghana as a case study which are placed into three (3) broad categories as: (a) regulators challenges including: (i) inefficient telecommunication fraud prevention policies (ii) lack of proper coordination and cooperation between implementation agencies, (iii) bureaucracy, (iv)infrastructure and technology deficit, (v) lack of skilled man power, (vi) the quest to earn high revenue in international termination fees to sustain economy and telecom operations, (vii) lack of financial resources to implement telecom policies, and (viii) political influence and corruption, (b) operators challenges are: (i) fear of losing customers, (ii) lack of political will or the laxity of regulators to implement and enforce telecom policies, and finally, (c) User/subscriber challenges namely: (i) lack of education and awareness, (ii) negligence and poverty.

In addition to the findings of previous studies by Michael L. Best and Dhanaraj [2] and Kanene Onyeajuwa [14] which stated that the implementation challenges of telecommunication (fraud prevention) policies in developing countries are: (a) weak institutions, (b) intra-governmental institutions actors, (c) the dominance of the elite groups in decision making, (d) limited understanding of policy process, (d) no special intervention to make basic mobile services accessible and affordable to low-income ordinary consumers and (e) the laxity of enforcing rules by regulators, the research found that (i) inefficient fraud prevention telecom policies, (ii) the quest to earn high revenue in international termination fees to sustain the economy and telecom operations and (iii) lack of proper coordination and cooperation between implementation agencies, are the new challenges which were not previously stated as the challenges to the implementations of fraud prevention telecom policies. This does not discount the fact that some of the previously revealed challenges still exist.

The analysis of the data from the Ghana Police Service CID Unit confirms that there is a high rate of cybercrime, also known as telecom fraud in Ghana, of which just a small fraction (less than 20%) has been reported. The greater fraction is not reported for various reasons ranging from, lack of education, awareness or knowledge of where to report incidence, ignorance, through no fault of the victims but failure on the part of authorities responsible for helping them fight the crime.

A form of physical security trainings should have also been given to mobile banking merchants as to how to ward off physical attacks from robbers if it is so expensive to offer merchants physical security.

It is internationally recognised that, the application of international standard best practices is one of the ways to solving known problems. This however, has been misconstrued by most institutions or governments to serve as grounds for laziness as most always do what is popularly known as “Cut and Paste (**CP**)” method, meaning, the international best practices are often taken literally and applied to their given situations. This often fails, because practitioners of the “CP” method often forget that their culture, educational level, the geographic setting and level of technology are not the same.

For example, the use of short code system for emergency contacts works perfectly in the advance countries because: (i) there is a good level of education of citizens there, (ii) they have a common local national language which aids in the understanding of the less educated or uneducated ones on events, (iii) they have advance technology, and (iv) there is sufficient level of security awareness.

In Ghana and most developing countries however, the national language is a foreign language (example, English Language or other, depending on their colonial master) while the citizens speak many different ethnic languages and dialects. They also have different cultures. Majority of the subscribers little or no formal education. Therefore the application of short code system as emergency contact as is done in the advanced world will obviously not work well because an uneducated person will hardly remember an emergency short code to use to call to alert authorities when being or defrauded if even such emergency institutions exist.

The practice of "**CP**" in developing countries should be stopped and be replaced by a "Take, Modify and Apply (**TMA**)" to suit their cultural settings, level of education and technology. This could be done by decentralising the incident response unit to the local (District) levels with the help of operators and providing contact persons (officers) who could attend to complains of subscribers. This could also be done in parallel alongside the use of the short code system.

Decentralising the incidence response units/centres broadens the access level of subscribers in reporting crimes, increases reporting, security awareness as well as responses to crime levels. This also shortens response time. Aside that, ease of contact is also achieved by decentralising the incident response units, it will also create jobs for the teaming unemployed youth forced to conduct these frauds for survival.

Laws and regulations, different telecom laws and regulations practice by different developing countries constitute a big challenge in tackling inter border related telecom or cyber frauds. This lack of coordination and cooperation between inter regulatory bodies of member countries is a major setback in managing and curbing telecom and cyber frauds as jurisdiction and extradition laws hinder the apprehension of criminals. Again, the existence of so many implementation agencies with lots of bureaucratic procedures and lack of well-defined roles makes it difficult and confusing in the handling of matters relating to telecom or cybercrimes among the many agencies.

Politicising institutions which were supposed to have been independent is weakening efforts regulators to enforce the implementation of telecommunication fraud prevention policies in Ghana. Again, giving employment preferences to political party sympathizers at the expense of the consideration of expertise and not involving ordinary citizen or subscribers in security policy design and formulations also weakens potent security policy formulations. Hence the ineffectiveness of telecommunication fraud prevention policies and the wide spread telecom and cyber frauds in Ghana.

Tackling **Pyramid Scheme and Mass Marketing Frauds**, the Bank of Ghana should intensify education and awareness of Pyramid Scheme and Mass Marketing Frauds and other financial related frauds to Ghanaian citizens. Also, work with the parliament of the republic of Ghana to revise and improve the financial transaction laws in Ghana so as to weed out fraudsters taking advantage of weak and out dated laws and financial policies. The police

service should also be well resourced and educated on criminal financial transactions so they can discharge their duties effectively.

Though few researches have been made in telecommunication fraud prevention policies, none in particular combines telecommunication fraud prevention policies and implementation challenge as a main research. Yet it was still possible to get the needed information to continue with the research. Video recordings of interviews conducted by Ghanaian journalist with cyber/telecom fraudsters both inside and outside Ghanaian prisons relevant to research topic were also taken as secondary data.

The research gap addressed in this research is "telecommunication fraud prevention policies and implementation challenges". Other research gaps identified during the literature review which are yet to be work on are stated in the future works under section 6.1 and the contributions of this research to existing research are clearly stated under section 6.3 of this research document. Some recommendations have been put forward which may help address the current challenges if put into use. These recommendations are in the recommendation section below.

Financial constraints, limited time available and the unwillingness to corporate by certain institutions (operators were not willing to cooperate) constituted the research limitations. The research only focused on the challenges in implementing fraud prevention telecommunication policies, the economic and security impact in developing countries using Ghana as a case study. This was done to facilitate deeper understanding and effective evaluations based on the findings.

Ghana is a developing country having multiple ethnic groups with different languages, culture, low economic resources, low levels of education and security awareness of subscribers as well as low level of technology. These features mimic most developing countries especially those in sub-Sahara Africa. The recommendations of this study, therefore, are applicable to other developing countries.

6.1 Future works

Below are some of the intended topics to be researched on in the future:

- The challenges of centralised telecommunication regulatory bodies among developing countries.
- Challenges of telecommunication security education as a fraud prevention policy.

6.2 Recommendation

To achieve a possible solution to current challenges in implementing fraud prevention telecom policies requires a combination of instruments which will include elements of self-protection by prospective victims of telecommunications related illegality, self-regulatory initiatives by the targets of regulation, traditional law enforcement or regulatory intervention by states. The following are recommended to Ghana and other developing countries to help curb the high rate of telecom fraud:

I. Information Security should be given a higher priority at both parliamentary and executive levels of successive governments in developing countries than it is currently.

II. Developing countries should institute a centralised regulatory authority to help coordinate both inter and intra regulatory authorities of member countries so as help curb inter-border telecom frauds.
III. The Ghanaian government should refine its fraud prevention telecom policy to make it more robust, efficient, effective and up-to-date.
IV. There should be enhancement of co-operation between regulators of different countries, between regulators and Communication Fraud Control Association (CFCA), between operators within a country, and between operators and CFCA to tackle telecom fraud.
V. Quarterly review of policies on telecom fraud to see how effective they are implemented as well as the impact on the level of telecom fraud.
VI. Developing countries should invent new strategies in raising revenue for the costly telecom equipment and operation, and lower the higher termination rate so as to discourage Simbox and OTT Bypass fraudsters.
VII. Developing countries should make use of the Near Real Time Roaming Data Exchange (NRTRDE) systems to help reduce the level of roaming fraud.
VIII. The communication channels for the various implementations agents in Ghana should be refined to reduce the levels of bureaucratic hurdles and be more transparent.
IX. Telecos/operators should be made to be more transparent in their pricing/charges and promotional dealings with subscribers so as to be more accountable to the government and citizens/subscribers.
X. There should be intensive public education and awareness training on telecom fraud
XI. Ghana government should incorporate information security educational syllables starting from the basic to the Senior High School level. This can also be done in collaboration with the National Commission for Civic Education (NCCE) which is already doing a similar education on the constitution and laws of Ghana.
XII. There should be a decentralisation of the government incidence response unit in all regional capitals and district levels in collaboration with the various operators for easy reporting of crimes and crime management.
XIII. Governments/regulators should provide incentives to people who voluntarily give tips to authorities to arrest fraudsters as this serves as a motivation to encourage citizens to take part in community policing.
XIV. Governments should create more jobs for the youth. This reduces the tendency to become a fraudster in order to have a livelihood.
XV. Above all, the Ghanaian citizens should try to avoid politicising everything including institutions which are supposed to be independent of political influence so that those institutions can carry out their mandates effectively including tackling corruptions and frauds.

6.3 Contribution

The research was able to make the following as our contribution;

1. Determined the causes of telecom frauds from the policy level as a result of the challenges in implementing fraud preventing policies.
2. Established that:
   I. inefficient fraud prevention telecom policies,

II. the quest to earn high revenue in international termination fees to sustain the economy and telecom operations and
III. lack of proper coordination and cooperation between implementation agencies.

3. The research highlighted some of the tricks of social engineering fraudsters in Ghana
4. Categorized the challenges facing Ghana in confronting the telecom fraud into formal (regulators challenges), technical (operators challenges) and informal (User/subscriber) challenges
5. Also, exposed some of the lackadaisical attitude towards enforcing policy on telecom fraud by both government and operators

6.4 Conclusion

The case of Ghana is not as unique as it is just a reflection of what is happening most developing countries world-wide especially sub Saharan African countries. Ghana though has made some progress in recent years, a lot still need to be done in particularly on telecommunication/ cybersecurity education and awareness.

In as much as the challenges of Governments are acknowledged, they needs to place higher priority on information security so as to move them away from being only reactive to a more assertive status and proactive in their dealings with telecommunication frauds and cybercrimes in general. This should also include the provision of jobs to the teaming unemployed youth who conduct frauds as a means of livelihood. The monies lost through these fraudulent activities yearly is enough to create employment for most of these unemployed youth.

An excellent telecommunication security policy is as good as its implementation. And good implementation of an excellent security policy is realised when there is a successive security education and awareness. Therefore, the success of an excellent security policies lies in the security culture of the citizens/subscribers. Its only when these are achieved that a security policy can be termed effective and efficient.

The negligence of the unemployed youth and the lack of telecommunication security/cybersecurity education for citizens by governments in developing countries like Ghana is very dangerous for the future. Most the unemployed youth feels their future is been stolen by greedy leaders/politicians by denying them jobs. And as such, the leaders in developing countries are not good examples to them.

Again, the politicisation of almost every sector including institutions which are supposed to be independent by Ghanaians weakens successive governments' efforts to tackle frauds. This includes the selective employments based on political party affiliations which at times is not based on competence thereby weakening proactive security designs, formulations and implementations.

Members of developing countries should try and improve their security sharing information, cooperate and coordinate more effectively to curb inter border related telecommunication frauds and other cybercrimes.

The current challenges in implementing fraud prevention telecom policies in developing countries using the country Ghana as a case study of which we broadly placed into three (3) categories which include: (a) regulators challenges as (i) inefficient fraud prevention telecom

policies (ii) lack of proper coordination and cooperation between implementation agencies, (iii) bureaucracy, (iv)infrastructure and technology deficit, (v) lack of skilled man power, (vi) the quest to earn high revenue in international termination fees to sustain economy and telecom operations, (vii) lack of financial resources to implement telecom policies, and (vii) political influence and corruption, (b) operators challenges as (i) fear of losing customers, (ii) lack of political will or the laxity of regulators to implement and enforce telecom policies, and finally, (c) User/subscriber challenges as (i) lack of education and awareness, (ii) negligence and poverty.

6.5 Significance of Study

This thesis assessed the current challenges in implementing fraud prevention telecom policies in developing countries for that matter Ghana and its corresponding negative impact on the country as well as provide alternative approaches by way of recommendations. The thesis is meant to also serve as a wakeup call on my fellow African researchers and researchers worldwide to re-look at what the real roots of the problems of cyber or telecom frauds by re-examining the institutions responsible for the detections and preventions of these frauds in Africa and the world at large

Reference

[1] Smith, K. and Larimer, C. (2016). *The Public Policy Theory Primer*. [online] Routledge.com. Available at: https://westviewpress.com/wp-content/uploads/2016/05/Public-Policy-Theory-Primer-Sample-Westview-Press-Fall-2016.pdf [Accessed 13 May 2018].

https://westviewpress.com/wp-content/uploads/2016/05/Public-Policy-Theory-Primer-Sample-Westview-Press-Fall-2016.pdf

[2]. Best, M. and Thakur, D. (2009). *The telecommunications policy process in post-conflict developing countries: the case of Liberia*. [online] Citeseerx.ist.psu.edu. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.462.4238&rep=rep1&type=pdf [Accessed 13 May 2018].

[3] Stone, D. (2002). *Policy Paradox: The Art of Political Decision Making*.

[4] Torjman, S. (2005). *What is Policy?*. [online] Vibrantcanada.ca. Available at: http://vibrantcanada.ca/files/what_is_policy.pdf [Accessed 13 May 2018].

[5] Republic, G. (2004). *National Telecommunications Policy*. [online] Researchictafrica.net. Available at: https://researchictafrica.net/countries/ghana/National_Telecommunications_Policy_2005.pdf [Accessed 13 May 2018].

[6]. IIDA, Y. (2011). *Japan's Telecom Policy and Infrastructure*. [online] Scholar.google.com. Available at: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Japan%E2%80%99s+Telecom+Policy+and+Infrastructure+by+Yoichi+IIDA%2C+2011&btnG= [Accessed 13 May 2018].

[7] Singh, H., Soni, A. and Kathuria, R. (2005). *TELECOM POLICY REFORM IN INDIA*. [online] Siteresources.worldbank.org. Available at: http://siteresources.worldbank.org/INTRANETTRADE/Resources/Singh.pdf [Accessed 13 May 2018].

[8] The European Union Telecommunications Policy by Mr. Erkki Liikanen and Sarajevo, September, 2001.

[9] Ogiemwonyi Arakpogun, E., Wanjiru, R. and Whalley, J. (2017). Impediments to the implementation of universal service funds in Africa – A cross-country comparative analysis. *Telecommunications Policy*, 41(7-8), pp.617-630.

[10] Xia, J. (2016). Universal service policy in China (I): Institutional elements and ecosystem. *Telecommunications Policy*, 40(2-3), pp.242-252.

[11] Madden, G. (2010). Economic welfare and universal service. *Telecommunications Policy*, 34(1-2), pp.110-116.

[12] Maddens, S. (2009). *TRENDS IN UNIVERSAL ACCESS AND SERVICE POLICIES: CHANGING POLICIES TO ACCOMMODATE COMPETITION AND CONVERGENCE*. [ebook] Available at: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/USPolicy.. [Accessed 13 May 2018].

[13] Srinuan, C. (2014). Uncertainty of public pay phone in Thailand: Implications for the universal service obligation. *Telecommunications Policy*, 38(8-9), pp.730-740.

[14] Onyeajuwa, M. (2017). Institutions and consumers: Assertion of ordinary consumer interest in the Nigerian digital mobile telecommunications market. *Telecommunications Policy*, 41(7-8), pp.642-650.

[15]. Ciosummits.com. (2011). *Telecoms Fraud Management -Who is winning the Battle? A Praesidium Business Consultancy White Paper*. [online] Available at: http://www.ciosummits.com/media/pdf/solution_spotlight/wedo_telecoms-fraud-management.pdf [Accessed 13 May 2018].

[16] Grabosky, P., Smith, R. and Wright, P. (1996). *Crime and telecommunications*. [online] Australian Institute of Criminology. Available at: https://aic.gov.au/publications/tandi/tandi59 [Accessed 13 May 2018].

[17] Pine, G. (2014). *Security Policy*. [online] Sotcstudent.net. Available at: http://www.sotcstudent.net/networksystems/wp-content/uploads/2014/04/Security-Policies.pdf [Accessed 13 May 2018].

[18] Instantsecuritypolicy.com. (n.d.). *The IT Security Policy Guide*. [online] Available at: https://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf [Accessed 13 May 2018].

[19] Republic, G. (n.d.). *Vision/Mission/Values - Ministry of the Interior*. [online] Ministry of the Interior. Available at: https://www.mint.gov.gh/the-ministry/about-us/visionmissionvalues/ [Accessed 13 May 2018].

[20] Cipfa.org. (n.d.). *The Chattered Institute of Public Finance and Accountancy (CIPFA)*. [online] Available at: http://www.cipfa.org/html/elearning/nasbm/fraud%20awareness/resources/frauddefinitionandexamples.pdf [Accessed 13 May 2018].

[21] Ag.gov.au. (2017). *Resource Management Guide No. 201 - Preventing, detecting and dealing with fraud*. [online] Available at: https://www.ag.gov.au/CrimeAndCorruption/FraudControl/Documents/FraudGuidance.pdf [Accessed 13 May 2018].

[22] Sahin, M. and Antipolis, S. (2017). *SoK: Fraud in Telephony*. [online] S3.eurecom.fr. Available at: http://www.s3.eurecom.fr/docs/eurosp17_sahin.pdf [Accessed 13 May 2018].

[23] Lehr, W. and Kiessling, T. (1999). *Telecommunication Regulation in the United States and Europe: The Case for Centralised Authority*. [online] People.csail.mit.edu. Available at: http://people.csail.mit.edu/wlehr/Lehr-Papers_files/LehrKiesslingTPRCVolume.PDF [Accessed 13 May 2018].

[24] Ivir.nl. (2014). *Any Colour You Like: the History (and Future?) of E.U. Communications Security Policy*. [online] Available at: https://www.ivir.nl/publicaties/download/1421.pdf [Accessed 13 May 2018].

[25] Feasey, R. (2012). *Global–local: European telecoms regulation in the 2020s*. [online] Oxera.com. Available at: https://www.oxera.com/Oxera/media/Oxera/downloads/Agenda/Agenda-11-Telecoms-regulation.pdf?ext=.pdf [Accessed 13 May 2018].

[26] Europarl.europa.eu. (2013). *laying down measures concerning the European single market for electronic communications and to achi eve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012*. [online] Available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2013)0627_/com_com(2013)0627_en.pdf [Accessed 13 May 2018]..

[27] Ec.europa.eu. (2017). *EU cybersecurity initiatives, working towards a more secure online environment*. [online] Available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf [Accessed 13 May 2018].

[28] El-Moghazi, M., Whalley, J. and Irvine, J. (2017). World radiocommunication conference – 2015: Reflections on Africa international spectrum policy. *Telecommunications Policy*, 41(7-8), pp.631-641.

[29] Documents.worldbank.org. (n.d.). *(WDR) 2016 - World Bank Documents & Reports - World Bank Group*. [online] Available at: http://documents.worldbank.org/curated/en/961621467994698644/pdf/102724-WDR-WDR2016Overview-ENGLISH-WebResBox-394840B-OUO-9.pdf [Accessed 13 May 2018].

[30] Siteresources.worldbank.org. (2012). *World Bank Group Strategy for Information and Communication Technology 2012-2015*. [online] Available at: https://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/WBG_ICT_Strategy-2012.pdf [Accessed 13 May 2018].

[31] Fredebeul-Krein, M. and Freytag, A. (1997). Telecommunications and WTO discipline. An assessment of the WTO agreement on telecommunication services. *Telecommunications Policy*, 21(6), pp.477-491.

[32] NJ, R. (2015). *2015_CFCA_Global_Fraud_Loss_Survey_Press_Release*. [online] Available at: http://www.cfca.org/pdf/survey/2015_CFCA_Global_Fraud_Loss_Survey_Press_Release.pdf [Accessed 13 May 2018].

[33] Anon, (2015). *Illicit Financial Flow Report of the High Level Panel on Illicit Financial Flows from Africa*. [online] Available at: https://www.uneca.org/sites/default/files/PublicationFiles/iff_main_report_26feb_en.pdf [Accessed 13 May 2018].

[34] Digital Single Market. (2015). *Telecom Laws*. [online] Available at: https://ec.europa.eu/digital-single-market/en/policies/telecom-laws [Accessed 13 May 2018].

[35] Nationaldailyng.com. (2016). *It's time to move forward on telecoms sector | National Daily Newspaper*. [online] Available at: http://nationaldailyng.com/its-time-to-move-forward-on-telecoms-sector/ [Accessed 13 May 2018].

[36] Akinsuyi, Y. (2014). *CPC, NCC Form Alliance to Curb Abuses by Telecoms Firms Logbaby*. [online] Logbaby.com. Available at: http://logbaby.com/news/cpc--ncc-form-alliance-to-curb-abuses-by-telecoms-firms_19376.html#.WvjA0peYPIU [Accessed 13 May 2018].

[37] Guardian.ng. (2016). *Subscribers task MNOs on improved services*. [online] Available at: http://guardian.ng/technology/subscribers-task-mnos-on-improved-services/ [Accessed 13 May 2018].

[38] Nca.org.gh. (2003). *National Communication Authority Act 1996 (Act 524)*. [online] Available at: https://nca.org.gh/assets/Uploads/National-Communications-Regulations-2003-L.I.-1719.pdf [Accessed 13 May 2018].

[39] Nca.org.gh. (2011). *Subscriber Identity Module Registration Regulations*. [online] Available at: https://nca.org.gh/assets/Uploads/Subscriber-Identity-Module-Registration-Regulations-2011-L.I.-2006-24th-Nov-2011.pdf [Accessed 13 May 2018].

[40] Jentzsch, N. (2012). Implications of Mandatory Registration of Mobile Phone Users in Africa. *SSRN Electronic Journal*.

[41] Bog.gov.gh. (2008). *Bank of Ghana Banking and Financial Laws of Ghana*. [online] Available at: https://www.bog.gov.gh/privatecontent/IDPS/banking%20and%20financial%20laws%20of%20ghana%202006%20-%202008.pdf [Accessed 13 May 2018].

[42] Grindle, M. and Thomas, J. (2018). *Public Choices and Policy Change: The Political Economy of Reform in Developing Countries. Merilee S. Grindle , John W. Thomas | Economic Development and Cultural Change: Vol 42, No 1*. [online] Journals.uchicago.edu. Available at: https://www.journals.uchicago.edu/doi/abs/10.1086/452072 [Accessed 13 May 2018].

[43] Imurana, B., Haruna, R. and Kofi, A. (2014). *The Politics of Public Policy and Problems of Implementation in Africa: An Appraisal of Ghana's National Health Insurance Scheme in Ga East Distric*. [online] Diva-portal.org. Available at: http://www.diva-portal.org/smash/get/diva2:984479/FULLTEXT01.pdf [Accessed 13 May 2018].

[44] Billingviews.com. (2013). *Subex Wholesale Fraud Management Survey 2013*. [online] Available at: http://billingviews.com/wp-content/uploads/delightful-downloads/2013/09/Subex-Wholesale-Fraud-Management-Survey-2013.pdf [Accessed 13 May 2018].

[45] Dataprotection.org.gh. (2012). *DATA PROTECTION ACT ,2012*. [online] Available at: https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf [Accessed 13 May 2018].

[46] N. A. Wasmi, "Telecoms regulator says Viber is 'unlicensed' in the UAE," September 2014. https://dl.acm.org/citation.cfm?id=2978334.

[47] Aicasia.org. (2015). *Smart regulation for OTT growth*. [online] Available at: https://www.aicasia.org/wp-content/uploads/2017/10/2017-OTT-Matrix-with-USABC.pdf [Accessed 13 May 2018].

[48] Johnson, M. (2012). *Demystifying Communications Risk*. [online] Google Books. Available at: https://books.google.se/books?hl=en&lr=&id=iUE3DAAAQBAJ&oi=fnd&pg=PP1&dq=M.+Johnson,+Demystifying+Communications+Risk:+A+Guide+to+Income+Risk+Management+in+the+Communications+Sector.+Ashgate+Publishing+Limited,+2012.&ots=IYu09HY6dD&sig=y1rz-Nn6hSqzlFEo_REDR4bhcmU&redir_esc=y#v=onepage&q&f=false [Accessed 13 May 2018].

[49] Google.com. (2012). *"Article 28(2) Universal Service Directive: A harmonised BEREC cooperation process - Consultation paper," Body of European Regulators of Electronic Communications*. [online] Available at: https://www.google.com/search?ei=18z4WqPEENKx0gW24L8I&q=%29+Universal+Service+Directive%3A+A+harmonised+BEREC+cooperation+process+-+Consultation+paper&oq=%29+Universal+Service+Directive%3A+A+harmonised+BEREC+cooperation+process+-+Consultation+paper&gs_l=psy-ab.3...696080.696080.0.696900.1.1.0.0.0.0.208.208.2-1.1.0....0...1..64.psy-ab..0.0.0....0.GF_S6KPoe_8 [Accessed 13 May 2018].

[50] Anderson, R. (2008). *Security Engineering*. [online] Google Books. Available at: https://books.google.se/books?hl=en&lr=&id=eo4Otm_TcW8C&oi=fnd&pg=PT12&dq=pdf++R.+J.+Anderson,+Security+Engineering:+A+Guide+to+Building+Dependable+Distributed+Systems,+2nd+ed.+Wiley+Publishing,+2008.&ots=gBDOzKaB8a&sig=X5EWf_TtqqfsRmaI5HbAbo0qicE&redir_esc=y#v=onepage&q&f=false [Accessed 13 May 2018].

[51] Ftc.gov. (2009). *"Negative option marketing workshop report," Federal Trade Commission*. [online] Available at: https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf [Accessed 14 May 2018].

[52] Telsis.com. (2015). *Protecting Against the Next Generation of Telephony Fraud, a Telsis White Paper*. [online] Available at: https://www.telsis.com/wp-content/uploads/2017/03/Telephony-Fraud-White-Paper.pdf [Accessed 14 May 2018].

[53] Transnexus.com. (n.d.). *Telecom Fraud Guide | TransNexus*. [online] Available at: https://transnexus.com/resources/telecom-industry-topics/telecom-fraud-guide [Accessed 14 May 2018].

[54] Syniverse.com. (n.d.). *Understanding the Global Threat of Mobile Fraud.*. [online] Available at: https://www.syniverse.com/assets/files/global_mobile_fraud_trends_report.pdf [Accessed 14 May 2018].

[55] Warner, J. (2011). *Understanding Cyber-Crime in Ghana: A View from Below*. [online] Scholar.harvard.edu. Available at: https://scholar.harvard.edu/files/jasonwarner/files/warner2011ijcc_0.pdf?m=1399029310 [Accessed 14 May 2018].

[56] Nikita, N. (2015). *Billing system's extension for fraud detection*. [online] Dspace.cvut.cz. Available at: https://dspace.cvut.cz/bitstream/handle/10467/61833/F3-DP-2015-NikulinNikita-Nikulin_Nikita-1.pdf?sequence=1&isAllowed=y [Accessed 14 May 2018].

[57] Sbs.ox.ac.uk. (2014). *Ghana National Cyber Security Policy & Strategy*. [online] Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Ghana_Cyber-Security-Policy-Strategy_Final_0.pdf [Accessed 14 May 2018].

[58] Sahin, M. and Francillon, A. (2016). *Over-The-Top Bypass: Study of a Recent Telephony*. [online] S3.eurecom.fr. Available at: http://s3.eurecom.fr/docs/ccs16_sahin.pdf [Accessed 14 May 2018].

[59] Dryburgh, L. and Hewett, J. (2005). *Network Routing*. [online] Google Books. Available at: https://books.google.se/books?id=5OCcBAAAQBAJ&pg=PA940&lpg=PA940&dq=L.+Dryburgh+and+J.+Hewett,+Signaling+System+No.+7+(SS7/C7):+protocol,+architecture,+and+services.+Cisco+press,+2005.&source=bl&ots=mCTMg8pezg&sig=A6jEh2vD5zEbr3KXc_aEYl_OAGM&hl=en&sa=X&ved=0ahUKEwjd7KjYt_rWAhVBQpoKHR0HDfIQ6AEIPTAC#v=onepage&q=L.%20Dryburgh%20and%20J.%20Hewett%2C%20Signaling%20System%20No.%207%20(SS7%2FC7)%3A%20protocol%2C%20architecture%2C%20and%20services.%20Cisco%20press%2C%202005.&f=false [Accessed 14 May 2018].

[60] revenues, 1. (2016). *New threat to mobile network operator revenues - Revector*. [online] Revector. Available at: https://www.revector.com/new-threat-mobile-network-operator-revenues/ [Accessed 14 May 2018].

[61] Sujata, J., Sohag, S., Tanu, D., Chintan, D., Shubham, P. and Sumit, G. (2015). Impact of Over the Top (OTT) Services on Telecom Service Providers. *Indian Journal of Science and Technology*, 8(S4), p.145.

[62] Fisher, K. (2011). *Fisher Investments on Telecom (Fisher Investments Press)* -. [online] epdf.tips. Available at: https://epdf.tips/fisher-investments-on-telecom-fisher-investments-press.html [Accessed 14 May 2018].

[63] Bhawan, M. and Marg, J. (2015). [online] Trai.gov.in. Available at: http://trai.gov.in/sites/default/files/OTT-CP-27032015.pdf [Accessed 14 May 2018].

[64] Moc.gov.gh. (2018). *About Us | Ministry of Communications*. [online] Available at: https://www.moc.gov.gh/about [Accessed 14 May 2018].

[65] Moc.gov.gh. (2008). *National Communications Authority Act 769*. [online] Available at: https://www.moc.gov.gh/sites/default/files/downloads/Ghana-National-Communications-Authority-Act-769.pdf [Accessed 14 May 2018]. [66] https://nca.org.gh/the-nca/what-we-do/ [67] http://nita.gov.gh/about-us/

[68] Afriwavetelecom.com. (2018). *Afriwave Telecom Ghana Limited*. [online] Available at: http://www.afriwavetelecom.com/ICH.html [Accessed 14 May 2018].

[69] New-ndpc-static.s3.amazonaws.com. (2016). *POLICE SERVICE ACT, 1970 (ACT 350)*. [online] Available at: https://new-ndpc-static.s3.amazonaws.com/CACHES/PUBLICATIONS/2016/09/04/POLICE+SERVICE+ACT,+1970+(Act+350).pdf [Accessed 14 May 2018].

[70] Ministry of the Interior. (2018). *Ghana Police Service - Ministry of the Interior*. [online] Available at: https://www.mint.gov.gh/agencies/ghana-police-service/ [Accessed 14 May 2018].

[71] Interpol.int. (2018). *Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL*. [online] Available at: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [Accessed 14 May 2018].

[72] Gupta, R., Kumar, R. and Bharadwaj, A. (2017). Mobile Banking System in India: Practices,Challenges and Security Issues. *International Journal of Computer Trends and Technology*, 43(1), pp.24-48.

[73] Gupta, S., Gupta, P., Ahamad, M. and Kumaraguru, P. (2016). *Abusing Phone Numbers and Cross-Application Features for Crafting Targeted Attacks*. [online] Arxiv.org. Available at: https://arxiv.org/abs/1512.07330 [Accessed 14 May 2018].

[74] Webster, J. and Watson, R. (2002). *A NALYZING THE P AST TO P REPARE FOR THE F UTURE : W RITING A L ITERATURE R EVIEW*. [online] Web.njit.edu. Available at: https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf [Accessed 14 May 2018].

[75] Yin, R. (2012). *Applications of Case Study Research*. [online] Google Books. Available at: https://books.google.se/books?hl=en&lr=&id=FgSV0Y2FleYC&oi=fnd&pg=PP1&dq=Case+Study+Research+Design+and+Methods+Second+Edition+by+Robert+K.+Yin&ots=4295PqskMl&sig=_zEbsZI2caxw305USSGrGiVukjc&redir_esc=y#v=onepage&q=Case%20Study%20Research%20Design%20and%20Methods%20Second%20Edition%20by%20Robert%20K.%20Yin&f=false [Accessed 14 May 2018]. Case Study Research Design and Methods Second Edition by Robert K. Yin, https://pdfs.semanticscholar.org/89c8/30dc397c4d76c8548b8f5f99def607798feb.pdf%20Robert%20K%20Yin&f=false

[76] Darke, P., Shanks, G. and Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal*, 8(4), pp.273-289.

[77] Rafael, G. (2007). *A Concept Map for Information Systems Research Approaches*. [online] Irma-international.org. Available at: http://www.irma-international.org/viewtitle/33198/ [Accessed 14 May 2018].

[78] Chen, W. and Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal*, 14(3), pp.197-235.

[79] Klein, H. and Myers, M. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, 23(1), p.67.

[80] Mitev, N. (2000) “Toward Social Constructivist Understanding of IS Success and Failure: introducing a new computerized reservation system”, Proceedings of the twenty fist

international conference on information systems, December, Brisbane, Queensland, Australia, pp. 84- 93.

[81] Watra.org. (2018). *About Us | West African Telecommunication Regulatory Assembly*. [online] Available at: http://watra.org/en_US/about-us/ [Accessed 14 May 2018].

[82] Sata-sec.net. (2018). *Committees*. [online] Available at: http://www.sata-sec.net/opencart/index.php?route=product/category&path=64_67 [Accessed 14 May 2018].

[83] BiztechAfrica. (2011). *Ghana to fight telecoms fraud*. [online] Available at: http://www.biztechafrica.com/article/ghana-vows-fight-telecoms-fraud/523/ [Accessed 14 May 2018].

[84] Hua, X. (2016). *Police, banks cooperate to fight telecom fraud|Government|chinadaily.com.cn*. [online] Usa.chinadaily.com.cn. Available at: http://usa.chinadaily.com.cn/china/2016-09/26/content_26893373.htm [Accessed 14 May 2018].

[85] Theubj.com. (n.d.). *Ukraine Telecom Rivals Unite to Fight Fraud*. [online] Available at: https://theubj.com/news/view/ukraine-telecom-rivals-unite-to-fight-fraud [Accessed 14 May 2018].

[86] Assets.publishing.service.gov.uk. (2013). *National Fraud Authority*. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf [Accessed 14 May 2018].

[87] Nyarko, W. (2017). *The Emergence of Mobile Banking in Ghana*. [online] Ghana Business & Finance Magazine - GB&F. Available at: https://ghanabusinessnfinance.com.gh/2017/02/24/the-emergence-of-mobile-banking-in-ghana/ [Accessed 14 May 2018].

[88] Ankiilu Kunateh, M. (2017). *Why Bank Of Ghana Fails To Act On Growing Mobile Money Fraud*. [online] Modern Ghana. Available at: https://www.modernghana.com/news/814371/why-bank-of-ghana-fails-to-act-on-growing-mobile-money-fraud.html [Accessed 14 May 2018].

[89] Gsma.com. (2013). *The Mandatory Registration of Prepaid SIM Card Users, a white paper*. [online] Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegistrationofPrepaidSIM-Users.pdf [Accessed 14 May 2018].

[90] Gsma.com. (2016). *Mandatory registration of prepaid SIM cards, addressing challenges through best practice*. [online] Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf [Accessed 14 May 2018].

[91] Donovan, K. and Martin, A. (2018). *The rise of African SIM registration: The emerging dynamics of regulatory change*. [online] Firstmonday.org. Available at: http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820 [Accessed 14 May 2018].

[92] kish, j. (2015). *Sakawa in Ghana*. [online] YouTube. Available at: https://www.youtube.com/watch?v=CmFEEmVY0MQ [Accessed 23 May 2018].

[93] Zimbi, A. (2014). *How Sakawa internet fraud turns into blood money*. [online] YouTube. Available at: https://www.youtube.com/watch?v=VEjRC47VT-M [Accessed 23 May 2018].

[94] Zimbi, A. (2014). *Sakawa Internet fraud experience in Ghana*. [online] YouTube. Available at: https://www.youtube.com/watch?v=Bi5oXVFANMo [Accessed 23 May 2018].

[95] Annafi, Y. (2015). *Sakawa tricks Boy Reveals with Amankrado*. [online] YouTube. Available at: https://www.youtube.com/watch?v=ypI0fXhqV1g [Accessed 23 May 2018].

[96] YouTube. (2018). *EXCLUSIVE INTERVIEW,PRISON INMATES ON DUPING SPREE #MobileMoneyFraudAlert*. [online] Available at: https://www.youtube.com/watch?v=hu1A0vaH07Q [Accessed 23 May 2018].

[97] Boy, G. (2016). *Ghanaian Scammer finally got caught pretending to be a woman*. [online] YouTube. Available at: https://www.youtube.com/watch?v=DluD90asKZw [Accessed 23 May 2018].

[98] Vision, 1FM. (2017). *LISTEN TO HOW SCAMMERS DOES THEIR JOB IN GHANA*. [online] YouTube. Available at: https://www.youtube.com/watch?v=PEGIu1ayi9g [Accessed 23 May 2018].

[99] Africa, V. (2018). *Well Known Sakawa Boy Finally Repents And Confesses - YouTube*. [online] YouTube. Available at: https://www.youtube.com/watch?v=lwjMJf7FLhs [Accessed 23 May 2018].

[100] YouTube. (2012). *Online dating scams fake webcams.flv*. [online] Available at: https://www.youtube.com/watch?v=vRx_fGwfdgo [Accessed 23 May 2018].

[101] YouTube. (2010). *Romance scam originated from Ghana led man to suicide - Africannewslive.com*. [online] Available at: https://www.youtube.com/watch?v=jmtO65_oUtQ [Accessed 23 May 2018].

[102] Krippendorff, K. (1989). *Content Analysis*. [online] Repository.upenn.edu. Available at: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1232&context=asc_papers [Accessed 25 May 2018].

Appendix

Research Plan

Below is the schedule plan for conducting my thesis;

Start date	Activity
November 2017: 20th November to 15th December,2017 17th December, 2017 27th December, 2017	- wrote proposal - first presentation of proposal - submitted initial thesis proposal
January 2018: 7th January,2018 25th January,2018	- re-submitted updated thesis proposal - final thesis proposal presentation
5th January, 2018 to 28th February, 2018 February-March 2018 1st to 9th February, 2018 12th to 16th February, 2018 19th February,2018 to 30th March, 2018 Within the same period 12th February, 2018 to 30th March, 2018.	- conducted literature reviews. - data collection: - presentation of an introductory letter from the university and a personal letter to regulatory institutions in Ghana introducing myself as a student and also seeking permission to conduct research/collect data for research respectively. - follow ups/scheduling interviews after receiving approvals from regulatory institutions. - administered interviews and questionnaire, this was done in a professional manner, questions were straight forward to avoid ambiguity and also polite to avoid intimation. - performed observations, this was done in a professional manner or passively to avoid obstructions to normal daily activities. The questionnaires were used when participants hardly find time to be interviewed as an alternative approach where necessary. Again, notes were taken during interviews and observations. - Further of analysis of data began while collecting data, this helped capture all required data.

17th March, 2018	- video recordings of interviews conducted by various journalist with telecom/cyber criminals both inside and outside Ghanaian prisons were also examined and analysed. Data Analysis: - further analysis of data - the analytic method to be employed in analysing data is content analysis with unit of analysis being country (Ghana). - drafting of report - submitted first drafted report
April 2018: 1st April, 2018 to 5th May, 2018 17th April, 2018	- drafting of report - submitted second drafted report
May 2018: 3rd May, 2018	- paj presentation of report/defence of thesis. - final presentation of report/defence of thesis.
June 2018	-

Research Questionnaire

LULEA UNIVERSITY OF TECHNOLOGY

Department Of Computer Science, Electrical and Space Engineering

Masters' Thesis Questionnaire

TOPIC: TELECOMMUNICATION FRAUD PREVENTION POLICIES AND IMPLEMENTATION CHALLENGES

This research work is seeking to examine the existing fraud prevention telecom policies, the challenges in implementing these policies vis-à-vis the existing telecom fraud. By responding to the questionnaire below you will help me identify some of the challenges faced in implementing fraud prevention telecom policies in Ghana.

1. What is the role of the National Communication Authority in regulating telecommunication operations in relation to cybercrime in Ghana?

……
……
……
……
……
……
……
……
……
……
……
……

2. What are some of the fraud prevention telecom policies in Ghana?

……
……
……
……
……
……
……
……
……
……
……
……

3. What are some of the challenges in the implementation of fraud prevention telecom policies in Ghana?

……
……
……
……
……
……
……
……
……
……
……
……

4. Do the various governmental institutions require to meet certain specified security assurance policies/standards before rolling out software packages for consumption? Yes / No
5. If No move to 7.
6. If Yes, what are the policies, and which body ensures its implementation?

……
……
……
……
……
……
……
……
……
……
……
……
……

7. What policy exist to ensure that various telecom companies engaging in banking assure citizens security?

……
……
……
……
……
……
……
……
……
……
……
……

8. What happens if a particular telecom company fails to abide by the fraud prevention policy?

……
……
……
……
……
……
……
……
……
……
……
……
……

9. Does your institution have an incident response unit to handle cybercrime in Ghana? Yes/No

10. If No move to 12

11. If yes, what are the figures of reported cybercrime in Ghana for the past five years?

……
……
……
……
……
……
……
……
……
……
……
……

12. What form of education on telecom fraud is giving to the Ghana Police Service and Citizens ?

……
……
……
……
……
……
……
……
……
……
……
……
……..

13. Does your institution provide any form of incentives to people who provide information about fraudsters to be arrested? Yes/ No