Geneva Business School®

Real Business. Responsible Leaders.

Research Paper

Assessing the effectiveness of the Amended Uganda Computer Misuse Act in addressing e-commerce cybersecurity risks: A case study of identity theft within MTN Uganda's Mobile Money e-services

Bachelor Thesis

Geneva Business School

Bachelor of Business Administration-Specialization in International Management

Submitted by: Grace Rachael ACAYO

06/06/2021

Supervised by: Biliana Vassileva

[XXXXXXXXXX]

Geneva, Switzerland

Date: [DD/MM/YYYY]

Word count: 9653

Declaration of Authorship

“I hereby declare:

- That I have written this work on my own without other people’s help (copy-editing, translation, etc.) and without the use of any aids other than those indicated;
- That I have mentioned all the sources used and quoted them correctly in accordance with academic quotation rules;
- That the topic or parts of it are not already the object of any work or examination of another course unless this has been explicitly agreed on with the faculty member in advance;
- That my work may be scanned in and electronically checked for plagiarism;
- That I understand that my work can be published online or deposited to the school repository. I understand that to limit access to my work due to the commercial sensitivity of the content or to protect my intellectual property or that of the company I worked with, I need to file a Bar on Access according to thesis guidelines.”

Date: 06/06/2021

Name: Grace Rachael ACAYO

Signature: Grace Rachael ACAYO

Acknowledgments

I take this opportunity to extend my heartfelt thanks to all my friends and family that have seen me through to this day. I greatly thank the women who supported me financially while undertaking this study in Geneva. I would also like to thank my supervisor for her leadership training, patience, and detailed guidance while guiding me to complete this thesis. I am also very grateful to the International Telecommunication Union for the opportunities, training, and support they provided when I developed this research plan.

List of Abbreviations

MTN	Mobile Telephone Network
ITU	International Telecommunication Union
A U	African Union Convention
SDGs	Sustainable Development Goals
GBS	Geneva Business School
USD	United States Dollar
CIRT	Computer Incident Response Team
U.S.	United States
U.K.	United Kingdom
ITC	Information and Telecommunication Communication

List of Tables

List of Figures

Table of Contents

Abstract

The problem of identity theft and cybercrime has become a serious challenge to most countries in the world. Most researchers are of the view that identity theft is a form of cybercrime. Although the origin of cybercrime is still unknown, it is now a global phenomenon.

At the heart of this, this research aims to study the effectiveness of the amended Computer Misuse Act of Uganda in providing mechanisms and a platform to enhance cybersecurity for businesses with e-commerce with a focus on telecommunication giant MTN Uganda mobile, specifically on the mobile money e-services. The researcher interviewed 10 MTN mobile users to understand their experiences and conducted a quantitative survey that received 58 responses. The research and interview helped determine the current identity theft experiences and techniques within MTN Uganda's Mobile Money e-services.

The research carried out has discovered that at least more than 70% out of 58 respondents using the MTN mobile money e-services have experienced identity theft. Findings of the research revealed that:

- Amon the 58 respondents, 14% of them realized that new SIM cards were registered in their names and full details;
- 69% of the 58 respondents were called by someone who requested a refund to money that was mistakenly sent to their account and;
- 3% believed that the mobile money agent/MTN staff colluded and robbed their mobile account, hence losing money.

This study conducted to check the effectiveness of the Uganda Computer Abuse Act found that through the results of desk reviews, interviews and investigations indicated that some articles in the Computer Abuse Act involved identity theft. However, most of them are general (covers all cybercrime) and does not go in-depth on how the Act is enforced and the amount of penalty given to liable criminals.

In this study, the investigation concludes that the Act should continuously be reviewed to enhance regulations on cybercrime, in particular, identity theft and recommends that there should be increased levels of policy awareness. MTN needs to conduct active knowledge sharing and alerts on identity theft methods among mobile money users to help them deal with identity theft challenges and active law enforcement at the MTN managerial level to be implemented.

Keywords: [Uganda Computer Misuse Act, Cybersecurity, Cybercrime, e-commerce, identity theft, MTN mobile money services]

1 Chapter One: Introduction

1.1 Background of the study

Within the international setting, cybersecurity in e-commerce engagement is one of the world's most urgent international business and e-commerce challenges (Price Waterhouse Coopers, 2021). The emergence of the COVID-19 pandemic has further propelled this. As a result, cybersecurity is currently among the world's top ten most potent risks (World Economic Forum, 2021) as a result of remote working and digital engagements, including e-e-commerce. With the ever-increasing digitalization of businesses, it is estimated that over 85 per cent of business organizations worldwide suffered a cybersecurity threat in the year 2020 (Sobers, 2021). The rise in e-commerce post-covid-19 pandemic is expected as businesses re-strategize.

At the regional level, some of the major initiatives to address e-commerce cybersecurity risks include the African Union (A.U.) Convention on Cybersecurity and Data Protection has managed to secure only 35 ratifications from the continent's 54 member states as of December 2020 (Baliño, 2021). At the national level, Uganda does not yet have a national cybersecurity strategy. Still, it has put numerous laws and regulations that address cybersecurity, including the 2011 Computer Misuse Act (as amended in 2017).

Uganda's revised Computer Misuse Act ensures the security of Uganda's electronic transaction and information systems, emphasizing the prevention of illegal access, abuse, and misuse of information systems, including electronic devices like mobile phones where many mobile money transactions occur.

Going by the above trends, there is a need to assess the role of the amended Computer Misuse Act towards addressing e-commerce risks associated with the telecommunications industry, including identity theft within the mobile money e-commerce business. A study (Mugoya, 2021) in Uganda assessing the adoption of e-commerce across Ugandan youth found that the primary reason for limited utilization of e-commerce services among youth was the high levels of cyber insecurity (lack of trust) within Uganda's digital landscape. Cyber threats and vulnerabilities are increasing trust issues within businesses and organizations globally (Wisseman, 2015-2021).

The utilization of cybersecurity frameworks to solve this will not only boost e-commerce businesses towards increased levels of profitability in a country where over half of its 45 million population are youth but also aid financial inclusion of this significant group of citizens that seeks to address the first Sustainable Development goals and ultimately the 2030 sustainable development goals as a whole.

1.2 Problem Statement

Cybercrime has become a nightmare that is increasing day by day. Cybercrime comes in different forms, such as phishing, malware attacks, fake identities to steal money or information, and other online scams. In a recent U.K. study, one in six adults are victims of online fraud or cybercrime (Experian 41st Parameter, 2021). In Uganda alone, it is estimated that cybercrime cost businesses 42 million USD a year (Serianu,, 2017)

This research study focuses on one aspect of cybercrime of identity theft. Identity theft is one of the fast-growing financial crimes around the world.

Since the dawn of the economic liberalization policy in the 1990s, numerous private sector strongholds have risen, including the country's largest company by revenue as of 2019, MTN Uganda. The company has suffered multiple cybersecurity attacks in the last decade because it holds over 80 per cent of the market share in mobile money (Stephen, 2020) and telecommunications digital financial transactions, boasting a huge profit margin compared to its competitors.

The high-profit margin MTN holds makes it a significant target by cybercriminals. One of the most common cyber-attacks on MTN Uganda's mobile business is identity theft among mobile money users. These problems have posed the following questions that will guide the study and thereby enhance the need for MTN to use the amended Computer Misuse Act to improve its mobile money services, hence building trust within its users.

1.3 Purpose of the study

This research is set to assess the effectiveness of Uganda’s amended Computer Misuse Act in addressing cybersecurity risks within MTN Uganda’s mobile money e-commerce business. The research was conducted within the timeframe of three months from March to June 2021.

1.4 Specific Objectives

- To gather the identity theft experiences of mobile money users while using the MTN mobile money services;
- To examine ways used by cybercriminals to steal MTN users to contrast and compare the effectiveness of the Act in addressing them;
- Lastly, to present recommendations for improving the Act and implementations on the enforcement part at the national and MTN level.

1.5 Research Questions

RQ1. How effective is the amended Computer Misuse Act in addressing cybersecurity risks within MTN Uganda’s mobile money e-commerce business?

RQ2. What are the several ways and manners individuals experience mobile money identity theft using MTN mobile money services?

1.6 Scope of the study

Subject scope

The study assessed the effectiveness of Uganda's amended Computer Misuse Act in addressing cybersecurity risks within MTN mobile money users.

The MTN of Uganda is a part of the MTN Group telecommunication company (GSMA, 2010) and since its launch in Uganda in 1998, MTN is by far the largest mobile telecommunications company operating in Uganda. Today, it has more than 3.5 million customers and provides GSM coverage for more than 90% of Uganda's urban population (GSMA, 2010).

The Uganda Computer Misuse Act was first enacted in February 2011 before it was amended in 2017. According to the Act, the purpose of the law is to provide requirements and regulations for the protection of electronic transactions and information systems; the law aims to prevent illegal access, use, or improper management of information systems. These system protections may include the use of computers to ensure that electronic transactions are conducted in a reliable electronic environment and to resolve other related issues (Guidance, Ministry of ICT and National, 2019).

Common forms of identity theft are from;

- Phishing, the use of false advertising and promotional activities, unsolicited scams mainly through email, where scammers pretend to provide and advise customer needs, promote false price increases and send money to imposters in the hope of receiving rewards (CGAP, 2017).
- Scam imitators call on consumers who claim to represent service providers to trick customers into revealing their mobile money account PIN or other personally identifiable information, thereby misleading customers. (CGAP, 2017).

According to Uganda National Information Technology Survey 2017/2018 report (The Collaboration on International ICT Policy for East and Southern Africa, 2018), a majority (70.9%) of all individuals owned a mobile. Among those who owned mobile phones, very few (15.8%) indicated that it was a smartphone. The report also reports that most (70.1%) people who owned mobile phones used them for sending and receiving mobile money. It further reported that MTN had the most users with 73.7% of individuals holding an MTN SIM card. This was followed by Airtel, that had 61.4% and Africell with 7.3%. (The Collaboration on International ICT Policy for East and Southern Africa, 2018)

Geographical scope

Uganda is an independent landlocked country located in Eastern Africa, obtaining its independence from Britain in 1962. Uganda is most often known and referred to as “the pearl of Africa”; the country is characterized by its magnificent physical features, including several endemic species and hosts the world's second-largest freshwater lake by volume – that’s the Lake Victoria. Uganda borders South Sudan to the north, Kenya to the east, Lake Victoria to the southeast, Rwanda to the southwest, and the Democratic Republic of the Congo to the west. The country's current coordinates are 1.3733° N, 32.2903° E.

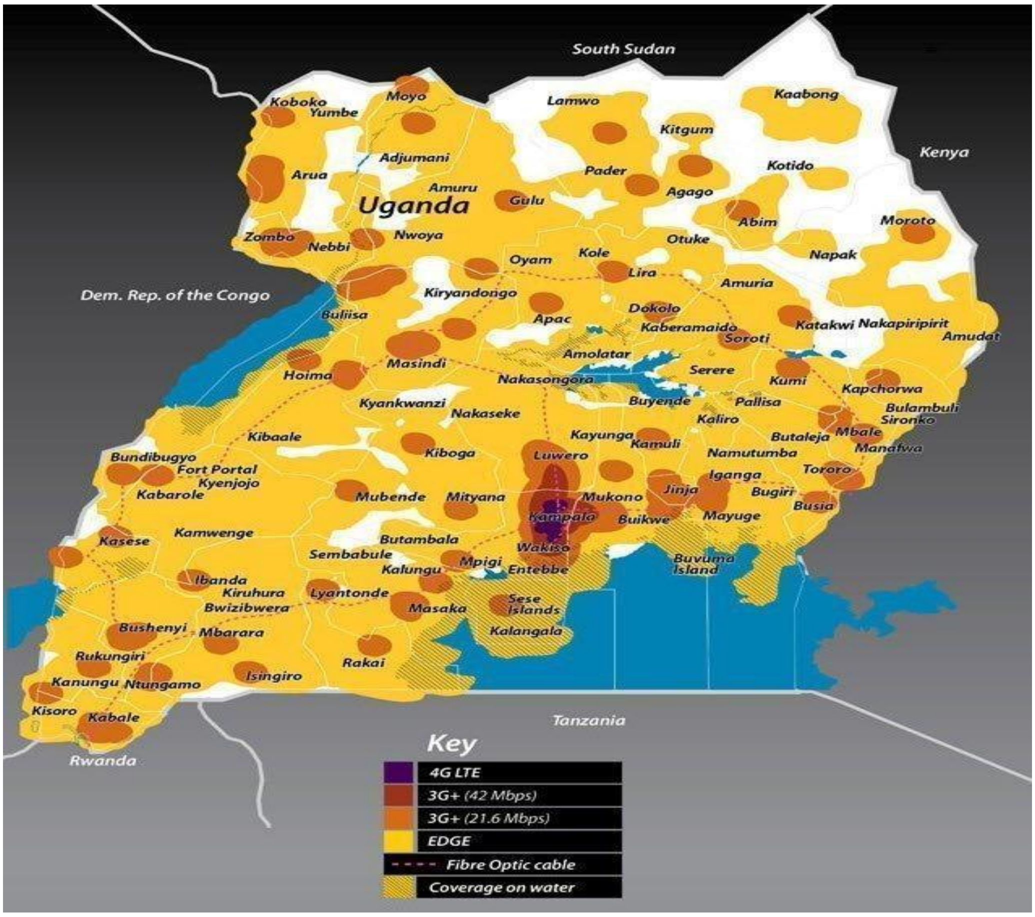

Figure 1: A map of Uganda showing MTN Uganda’s Network Coverage

Source: (Tech Jaja, 2015)

Study time scope

The study was limited to two years of information and ran for three months from April 2021 to June 2021. At the end of this period, the researchers will be able to submit a final report.

1.7 Justification of the study

Cybersecurity is an ever-growing threat to the financial services industry and businesses of all types, from small businesses to large corporations. According to a 2018 Ravelin Technologies Limited study, e-commerce businesses' identity theft, also known as payment fraud, accounts for 71 per cent of all scams experienced in the e-commerce business sector worldwide.

Uganda is no exception to this statistic. The e-commerce space has experienced a surge of cybercriminals committing fraud using several techniques such as phishing, keyloggers, credit card skimming, and others.

Because of these cybercrime concerns, the Ugandan government introduced the Uganda Computer Misuse Act (UCMA) in 2011. In addition to adopting new sections related to cybercrime, it amended the existing Computer Misuse Act in 2017. Security experts and tech media have praised this legal update as a significant international step that could help combat cybercrime in Uganda and the region.

1.8 Significance of the study

In October 2020, international media was flooded with news of MTN Uganda's mobile money system hack (Stephen, 2020). For a company that is the country's largest taxpayer and hosting financial transactions daily that amount to about 1 million USD, a cyber-attack offers an excellent risk for the company's operations. This was not the first of its kind; MTN has suffered several attacks before.

In a country where over 90 per cent of the cybercrimes remain unreported (Forensics Institute Uganda, 2018), an urgency to address cyber insecurity through solid government policy and commitment is required.

1.9 Conceptual framework

The study aims to examine the effectiveness of the currently revised amended Computer Misuse Act in addressing cybersecurity risks within MTN Uganda’s mobile money e-commerce business. The independent and dependent variables of this research include:

Table 1: Research Conceptual framework

Independent variables	Dependent variables
Role of cybersecurity Acts in addressing cyber risks	Effectiveness of cybercrime Act
E-commerce	Cybersecurity risks
	Current Cybersecurity policies

Source: self-constructed

The study is in line with the effect of Uganda's amended Cybercrime Act in improving trust and reducing identity theft within MTN mobile money services in Uganda. The independent variable, in this case, is the cybersecurity Act which looks at aspects like the role of cybersecurity Acts that lead to effective e-commerce performance. In this case, MTN mobile money performance seeks a better public image, effective service delivery, and trust. However, other factors, including the effective government policy, business culture, user experiences, and satisfaction, must be integrated for this to occur. In one way or another, all these lead to effective e-commerce services, which are brought about through the effective adoption of the Computer Misuse Act in MTN mobile money e-services.

1.10 Thesis structure

The structure of this research work is as follows:

1. Chapter one of this paper will explain the background of the study, the purpose of this study, its scope, justification, and significance of the study. It further explains why it is crucial to examine the effectiveness of the Uganda Computer Act in addressing identity theft in MTN mobile money services by developing questions that will be used to guide the research topic.
2. Chapter two will discuss the literature review of the different scholars and also collect information from various sources about the different terms used in the research. The literature review is explained in a logical order starting from the broad terms to the last terms as follows in the research topic: What is effectiveness, what is an Act, The Uganda Computer Misuse Act, the definition of cybersecurity, Business cyber risks, identity theft and how identity theft happens. This chapter also explains E-commerce, what MTN is, what mobile money is. It further describes researchers views on the role of policies and laws, including views on each of the terms mentioned.
3. Chapter three will discuss research methodology, including types of different data collection methods used. The chapter will start with the rationale and the justification for choosing the research design and methods. Also, the discussion will be related to the appropriate use of the different methods of data collection applied in the context of this study.
4. Chapter four will discuss results and analysis, separating them into objectives 1, 2 and 3 and discussing the findings.
5. Chapter five will discuss the conclusion, limitation of the study and recommendations of the researcher. This chapter is based on the findings of objectives 1, 2 and 3 to inform the readers if the Act is effective or not.
6. References and appendixes used will be provided at the end of chapters five.

Hence, the structure developed in this thesis supports evaluating participant perspectives. Findings were analyzed in relation to the existing knowledge of the different researchers to demonstrate how this research contributes to expanding the knowledge base.

2 Chapter Two: Literature Review

This chapter explores an extensive literature reviews of different scholars, research studies published in relation to terms used in this research paper such as effectiveness, cybersecurity and cybercrime, e-commerce, identity theft, cybersecurity acts as a distinct domain of the study and their relevancies and importance within businesses.

2.1 Definitions of Terms

This subchapter introduces all the key terms that the study uses throughout this thesis, explained logically as indicated in the research topic.

What is effectiveness?

A simple definition of effectiveness is that an activity or aspect should be able in fulfilling the purpose it was intended to do. (Harvey, 2004-2020). An Act, law or policy is only effective if it meets the following conditions: 1) it should be open and known to its community and public, 2) it should be acceptable by the community, 3) easy to be enforced, 4) balanced, 5) should be adoptable and modifiable, 6) remains constant, and 6) be able to solve disputes (Wilson, 2013).

Effectiveness expresses the extent to which legislation is conducive to the desired regulatory effects and the extent to which the attitudes and behaviours of target populations correspond to those prescribed by the legislators (Maria, 2014). Alternatively, effectiveness in law can be expressed as the extent to which the law can do its intended job and is supposed to be the primary expression of legislative quality (Maria, 2014).

What is an Act?

According to the U.K. Parliament (UK Parliament, 2021), “an Act creates a new law or changes to an existing law. It is a bill which has passed through the various legislative steps required for it and which has become law” ((Ministry of Justice and Constitutional Affairs, 2014)

The Uganda Cybercrime Misuse Act

The Uganda cybercrime Misuse Act (Parilament of Uganda, 2011) was first adopted in 2011 to protect Uganda from all forms of cybercrime. It should be noted that the Act was enacted subsequently due to the growing cases of cybercrimes in the country. As a member of the International Telecommunication Union and a signatory to the International Convention on Cybercrime, the government is committed to fighting criminal activities carried out through information networks. The Act accordingly provides for offences relating to cybercrime.

Cybersecurity

According to the ITU, cybersecurity can be described as "a set of tools, security policies, security specifications, security standards, guidelines, risk management methods and different approaches, activities, training, best practices, guarantees and technologies that can be used to protect network environment, organizations and user assets " (ITU-T X.1205, 2021). Many organizations, companies and small businesses information such as “connected computer devices, personnel information, critical infrastructure, applications, industries, ICT systems, including transmitted and stored data in the cyber environment all require healthy cybersecurity” (ITU-T X.1205, 2021). More so, cybersecurity endeavors to be committed to protecting the realization and maintenance of the organization's security attributes and user assets from the impact of related security risks in the cyber environment. (ITU-T X.1205, 2021). General cybersecurity objectives consist of Availability, Integrity that encompasses the authenticity and non-repudiation and Confidentiality (ITU-T X.1205, 2021).

Developing Countries, particularly Least Developed Countries (LDCs), are often less well-positioned to address cybersecurity challenges due to a lack of local capacity, resources, policy frameworks, research ecosystems, and political will. These are also countries where many new internet users will be coming from over the next decade.

Business Cyber risks

Globally, the primary business cybersecurity risks include ransomware, a form of malware that encrypts data and then seeks a ransom to unlock vital organizational data. Secondly, phishing involves attempting to gain access to sensitive information while posing as a trustworthy individual. With this insider threat, the staff of organizations is lured into providing sensitive data to outsiders. Hacking involves access to organizational data and information while not a member of the organization/from outside the organization. Finally, data leakage affects illegal access to data unconsciously left in the open access (Institute of Chartered Accountants in England and Wales, 2016).

Additionally, a 2017 Deloitte conference paper presented at the Next 2017 event; highlighted the urgency among business executives to deal with mobile money cyber threats as one of the ten most crucial cybersecurity issues in the global business world while advocating for leadership involvement to address cyber business threats (Deloitte, 2017). Interestingly, (Broadcom, 2016) found that email malware was the most common cyber-attack and risk for existing African medium and large-scale business enterprises on the African continent in 2015. The report reported an increase at a rate of 53 and 60 per cent in 2015 and 2014, respectively, costing African businesses and economies over 5 billion USD annually (Broadcom, 2016).

Furthermore, in a Serianu (Serianu,, 2017)study in 2018, ransomware was the most common cyber-attack in 2018 across the African continent. Numerous countries registered multiple private and public sector ransomware attacks (Association of Chartered Certified Accountants, 2019). Also, mobile financial transactions are the most prominent targets by cybercriminals. The mobile financial services industry registers the highest number of cyber risks culminated into attacks in the year 2019 within the Sub-Saharan region. This region also hosts the most significant number of mobile financial transactions globally on an annual basis (Open Access Government, 2020).

Additionally, (KnowBe4, 2020) report found that over half of Africans did not have the cyber threat basic knowledge making the cyber risk the most vulnerable to the working and elite African community. Although Africa has the most negligible damages registered from cyber-attacks, it has the world's highest cyber risk per capita than anywhere globally. Organizations based in Morocco, Namibia, Zambia, and South Africa are the most targeted continent-wide (OXial, 2020).

Furthermore, business leaders have finally identified that cybersecurity will be among the top 10 risks globally in 2021 through 2030 (Global consulting firm Protiviti and North Carolina State University Poole College of Management's Enterprise Risk Management (ERM) Initiative, 2021). According to the article, it appears that "cybersecurity and privacy threats will remain at a constant increase and should be at or near to the top of the list in the near future" (Global consulting firm Protiviti and North Carolina State University Poole College of Management's Enterprise Risk Management (ERM) Initiative, 2021)

Identity Theft

Identity theft can be defined as "a fraud or any other unlawful activity where an identity, i.e.a name, a document, or other identifying data is used to commit another crime, for example, credit-card fraud" (The United States Department of Justice, 2020).

Africa is one of the continents with a pronounced identity theft threat in the mobile money industry. This is partly because many African countries have limited/or do not even have laws and responsible agencies to deal with major identity theft threats. Additionally, many governments tend to unrecognize the right to personal privacy, thus not adopting regulations or put rules in place to observe the misuse and abuse of identity theft. Although the limited privacy protection system not long ago may not have attracted people's attention, the boom in mobile money adoption in Africa has dramatically increased the risk for consumers operating in an unprotected environment.

Despite the growing significance of mobile money in the Ugandan economy, identity theft remains a critical security challenge experienced by users. According to Ali *et al.*, (Ali, 2020), in an assessment study, found that 34.7% of respondents reportedly fully agree that identity theft is one of the system's security challenges of mobile money..

How does identity theft happen?

Most mobile money identity theft cases happen when a dishonest member of the mobile money staff/agent knows the PIN of a client. He/she can carry out unauthorized transactions (United States Homeland Security Science and Technology Division, 2018). Another common form of mobile money identity theft occurs when a customer's mobile phone is stolen. The thieves can use any sensitive data stored in it, including the PIN, and control the device.

.

E-Commerce

E-commerce can be defined as the sales of goods through the internet (Saimunur, 2014). E-commerce has a wide range of benefits, including better product information, more pricing information, service availability, lower communication costs, online technical support, quick response to customer requests, personalized orders, and virtual storefronts. visible to all Internet users. Reduce transactions. costs, shorten the purchase cycle, flexible pricing, reduce delivery costs for digital products and services, and allow customers to track orders (Valdeci et al., 2017).

Although e-commerce has brought great benefits, many small and medium-sized enterprises in developing countries, including Uganda, have failed to tap into e-commerce or achieve the setting required to realize the benefits associated with e-commerce. This is because there are many factors inhibiting adoption of e-commerce among both suppliers and customers and these include the high cost of initial investment, lack of developed legal and regulatory system, insufficient knowledge about e-commerce technologies, resistance by people and cultures, lack of right technical skills, too high financial risk, lack of standard business conduct, lack of awareness in ICT and e-commerce among others (Antoney, 2014).
According to the International Trade Administration of the U.S., despite informal and lax regulation, Uganda's e-commerce continues to grow rapidly due to the widespread use of mobile money (phone-based financial transfers) and the rapid expansion in the use of mobile phones. (Association, 2020).

According to the Report of the National Technology Survey of Information Technology of Uganda, the main form of (94.3%) among E-PayTing users was the transfer of mobile phone to mobile phones (The Collaboration on International ICT Policy for East and Southern Africa, 2018). This means that bank to mobile phones transferred (2.9%) followed mobile to mobile transfer (The Collaboration on International ICT Policy for East and Southern Africa, 2018). Suppliers are generally selling their products and services with consumers and sellers, and then connect with physical meetings. Payment generally carried out by cash or transfer of mobile money.

What is MTN?

MTN is a Mobile Telecommunication Network that is spread throughout Africa. It is estimated that more than 560 million Africans are covered by high-speed digital highways, and more than 30 million Africans have MTN Mobile Money in their pockets. (MTN Group Management Services , 2019).

Mobile Money services

The WorldRemit (WorldRemit, n.d) defines MTN mobile money as “a secure electronic service that allows MTN mobile money wallet holders to store funds, send and receive funds, make payments, and perform many other transactions using only their mobile phones. It's fast, simple, convenient, and reasonably priced. Furthermore, it is provided by MTN in cooperation with more than 10 cooperative banks in many African countries ”. According to GSMA (GSMA, 2010) This service is primarily used for those who do not have bank accounts in many developing countries.

Mobile money services were first introduced in Uganda by MTN in 2009, following the successful implementation of M-Pesa in Kenya (Baganzi et al., 2017).

2.2 Cybersecurity policies (Acts or laws) and the role they play in addressing cybersecurity risks.

A research analysis (McAfee, 2020) suggests that the significant role of cybersecurity policies in addressing cyber-attacks is to create critical points of focus for cybersecurity personnel within the organization. The study emphasizes the need to avert from the beliefs of a one-size-fits-all approach in global cybersecurity policy-making but instead adopt a needs-based approach to enhance effectiveness once adopted into businesses in a given environment. Also, the Australian government (Australia Government. , 2020) advises interested and aspiring business investors seeking opportunities within the Australian economy to follow protocols established within its cybersecurity policy guide. The government emphasized that the role of the country's cybersecurity policy is to enable all based operating in Australia to prepare the required resources needed to mitigate or adapt towards business cyber-attacks, in turn, building on business resilience to cyber-attacks (Australia Government. , 2020).

Cybersecurity policies also facilitate businesses to determine vulnerabilities within their information systems to address and commercialize these cybersecurity solutions, especially as a critical note point for business research and development teams (KPMG, 2021). More so, cybersecurity also helps in determining the country's feedback mechanism. Cybersecurity policies also enable cybersecurity experts to establish cybersecurity technical and potent solutions to deal with a company's cyber risk while offering a harmonized effort across all departments and interconnected systems cross-cutting different facets of an organization (Courchesne, 2021).

Another important role of cybersecurity policy in addressing cyber risks is that they provide regulatory agencies with the platform to develop models to balance accounting and reporting of cybersecurity engagements. These include incident reports while at the same time ensuring data sensitivity concerns are considered while addressing, protecting against, or investigating cybersecurity incidents as they happen (United States Homeland Security Science and Technology Division, 2018).

3. Chapter Three: Research Methods

In addition to discussing the populations and sample configurations that meet the criteria of the case study, this chapter will also describe in detail the study design and the methods used to collect data. The overall goal is to conduct an objective and credible investigation. This chapter also explains the stages the investigation goes through to obtain the necessary information. Also, in this chapter, the researchers describe the research area, the sample size, the data collection methods, and the measurement of variables.

The chapters present the quality criteria taken for the case study and the subchapters. Subchapter 3.1 details the research design, 3.2 to 3.5 elaborates how this study attempted to meet these criteria: Subchapter 3.2 defines what a case study. Its subsection further explores the case study in question. 3.3 explores the Socio-demographic and economic characteristics, while 3.4 illustrate the sampling techniques and procedures used. 3.5 and its sub-sections explains in detail the data collection methods used and criteria taken into consideration. Subchapter 3.6 admits limitations that are inevitable and need to be addressed to create transparency.

3.1 Overview of the Research Design

The researcher uses a case study design to gather data for the research. Yin (Yin, 2014) defines a case study as a research method that can produce a deep and multifaceted understanding of complex problems in real life. A case study can also be regarded as an intensive analysis of an individual unit or event stressing developmental factors concerning context (Bent, 2011). This design approach encourages the researcher to look at each phenomenon from multiple perspectives. One main objective of using this study design is to uncover unique characteristics and outcomes and identify patterns in the data (Creswell, 2013).

To achieve the research objective of the case study, the researcher uses desk review from observations obtained through examinations of documents such as; journal articles, books, academic theses, and working papers.

Further, to compile information on the experiences of MTN users who have faced identity theft while using MTN mobile money services, the researcher applied primary data collection through:

A. Interviewing 10 people to collect data to get in touch with users, get their experience and design the survey.

B. Conducted a survey (Questionnaire) with 58 respondents across all occupation types to determine the current identity theft experiences and techniques within MTN Uganda’s Mobile Money e-services.

Sub-sections below explain all the research methods used in this research by first looking into the case study that built this research.

3.2 Case study

A case study can be considered as "one of several ways to investigate whether it is related to social science or even society, because it aims to understand humans in a social context by interpreting human behavior as a single group, community, or single event. (Slide Share, 2015). It is a method used to divide a broad field of research into subjects that are easy to study. It can create a naturalistic context in which to analyze real-life occurrences, providing a holistic view of the studied phenomena (Merriam, 1998). With their inductive analysis and theory building approach, case studies can be applied successfully to education research (Merriam, 1998).

The basic perception of case study research is that it is an open-ended design, suitable for an exploratory study of a single authentic case. The researcher chooses to use this type of case to explore and selects those aspects of the case that will provide the most insight into its complex nature.

The case study in question

The research design of this study is descriptive and explanatory (Thomas, n.d.) case study that is examined mainly through qualitative methods with the support of a quantitative survey.

According to Thomas (Thomas, n.d.), qualitative researchers tend to analyze their data in general. In descriptive and explanatory case studies, researchers analyze explanations and theories about the phenomenon in the context of a theoretical framework (Thomas, n.d.).

The case study, in this case, will help the researcher concentrate the time to carry out a more in-depth study and identify the phenomenon's meaningful trends and patterns, rather than spreading thin and missing out on some of the fundamental issues (Nachmias et al., 1987). Instead of keeping to a broad topic on cybercity policies and risks in general, the researcher narrows down the topic to one type of cybersecurity risks (identity theft) within one operating section of the MTN – mobile money services.

Two primary data collections support this case study. The first one; by interviewing 10 people to make a qualitative analysis. The second; by serving 58 people to collect primary data for quantitative analysis.

3.3 Socio-demographic and economic characteristics

Demographic of MTN

Out of the 45 million residents in Uganda (World Bank, 2020), about 22 million registered mobile money users are out of the 24 million registered mobile phone users, which is over three times more than registered bank account holders. On an annual basis, the country reports about 17 billion USD in mobile money transactions, implying that about half of the country's GDP is transacted over mobile money services at some point in the financial year (Francis, 2018).

Currently, MTN holds the largest market share of mobile money transactions at 80 (Stephen, 2020) per cent in a country. These transactions are aided by over 200,000 mobile money transaction agents (Uganda Communications Commission, 2020). **A map of Uganda showing MTN Uganda's Network Coverage** illustrates the coverage of the MTN network in Uganda.

Social Demographics of participants

In May 2021, the researcher interviewed 10 mobile money users across Uganda, and 58 other users were tasked to fill in the questionnaire towards meeting the research objectives. Snowball sampling (Naderifar et al., 2017) is used to choose respondents for both qualitative and quantitative data collections. According to (Naderifar et al., 2017), when samples with objective characteristics are not readily available, snowball sampling is used. For this research, this method was chosen because it is cost-effective and time-saving since the respondents were obtained via primary data sources and the researcher not living within the country.

All the interviewees were Ugandans for the research participants, and many of the survey respondents were also Ugandans. Only a few survey respondents were foreigners. Participants are mixed men and women between the ages of 21 and 63. All occupations include government officials, banking, retail sales managers, small business owners, students, unemployed, etc. Most respondents had spent a long time using mobile services (at least more than five years). Many of the respondents' users used the mobile money services at least once a week to send money for transactions connected to their work and Personal transactions (family, friends, etc.). For more details on the demographics of respondents, refer to **Appendix 2: Socio-economic and demographic characteristics of the respondents sampling techniques and procedures.**

3.4 Data Collection Methods used

This section describes data collection methods used in the research to gather information on the experiences of MTN users who have faced identity theft while using MTN mobile money services. In the first place, the researcher has used desk review to gather secondary information from materials that are readily available to the scholar to create a data-based argument. Secondly, the researcher used qualitative and quantitative data collection methods to collect primary data through interviews and surveys. To analyze these data, the researcher has used content analysis (Mayring, 2004).

Owing to the research ethics, a confidentiality clause was adapted for all primary sources of data and several secondary data obtained, meaning the details of respondents and information will be anonymous.

All the research methods used are explained below in the respective logical order of Desk review, Qualitative research, and the quantitative research method as applied in the research.

3.4.1 Desk Review Research method

To achieve the research objective, extensive desk research covering official sources of publicly available information that are valid, voluntarily shared, were reviewed. Scholars reviewed research from numerous scholars, and official/authoritative sources were collected, including Uganda's Parliament Knowledge Sharing site.

In selecting the method of desk review, the researcher decided to use a variety of government reports, studies and surveys. The reports were downloaded from different government websites such as Uganda Parliament. The researcher also accessed the ITU website, which enabled her to search for the different study documents and reports published in academic journals.

Through these tools, connections were drawn to determine how the different pieces of information on the literature review related to each other and ultimately help create better solutions on the research topic.

This method provided support to the researcher in collecting data to determine the information needed to build up the argument on whether the Uganda Computer Misuse Act effectively addresses identity theft within the MTN mobile money services.

The desk review was supported by conducting the interview and a survey, as explained below.

3.4.2 Qualitative Research method (through the interview)

Primary qualitative research was conducted through a series of interviews within all occupations. Questions were developed, and a snowball sampling (Naderifar et al., 2017) was used to find participants as they were randomly selected among MTN mobile users in Uganda.

The interviews were collected to understand the identity theft experience of MTN mobile money users to support the research topic. “the effectiveness of the amended Computer Misuse Act in addressing Identity theft within MTN mobile money e-services”. A total of 10 participants were interviewed, and the interview were conducted through phone calls where respondents answered closed-ended and open-ended questions.

The aim of conducting these interviews was focused on collecting data to inform the research. Based on content analysis (Mayring, 2004), the researcher used the information to design questions and answers to the questions, which were then used as a survey for quantitative analysis.

The methods used to ensure data quality control, the procedure taken, and data analysis applied in the qualitative research are described through three main subsections below:

- **Data Quality Control of Qualitative Research**

Questions were developed around the research objective and administered to interviewees. The interviews were developed using semi-structured (Lisa, 2008) questionnaires that focused on qualitative data. These questions were also tested and re-tested for clarity as the questions went through rounds of changes to fit the purpose of the research. They were administered to respondents on an individual basis independently to gather information and their suggestions.

- **The procedure of Qualitative Data collection**

The researcher scheduled time for each interviewee, starting with a few networking circles then using a snowball method of random interviewees introduced by the first interviewees.

The interviews were conducted using Otter, a transcription APP that transcribed all the live discussions that enabled vital information to be captured. After the interviews were conducted, a selection of relevant information was coded, catalogued and interpreted, as shown in **Appendix 3: Result from Interview.**

- **Data Analysis of Qualitative Research**

Then qualitative data was analyzed using Content analysis (Powers et al., 2010). (Powers et al., 2010) define Content analysis as a general term for several different strategies used to analyze text. Other researchers refer to content analysis "used to explore large amounts of textual information cautiously to determine trends and ways of using text, their frequency, their relationship, and the structure and communication of discourse system encoding and classification methods" (Mayring, 2004).

The findings were compared with quantitative data to draw a conclusion on the effectiveness of the amended Computer Misuse Act.

3.4.3 Quantitative Research Method (through Questionnaire survey)

The quantitative research was created as a result of the qualitative interviews conducted. A questionnaire was developed using critical themes from the qualitative interviews and was designed and performed using google forms for two weeks. The research started with five people known by the researcher and then shared with random people. The survey was posted on the researchers GBS google account. The survey, as designed, was anonymous; 58 responses were received.

For this research, 58 participants were selected randomly using snowball sampling techniques (Naderifar et al., 2017) from voluntary users of MTN mobile money services in Uganda.

The quantitative data collection was conducted to provide information to the assessment of objective two: To determine the current identity theft experiences and techniques within MTN Uganda's Mobile Money e-services.

The methods used to ensure data quality control, the procedure taken, and data analysis applied to the quantitative research are described through three main topics below:

- **Data Quality Control of quantitative Research Method**

All research methods complemented one another. The questionnaire as part of another primary data collection was also discussed with research supervisors. They were also tested and re-tested for accuracy with several trials of the survey by the researcher. Respondents were limited to one submission to control the quality of data collected.

- **The procedure of Quantitative Data collection**

Since this data was mostly collected from the questionnaire, the researcher created an online survey through google forms questionnaires and where respondents were delegated to fill in the survey.

- **Data Analysis of quantitative data**

Quantitative analysis extracts inductive reasoning from the data and distinguishes the phenomenon of interest from statistical fluctuations in the data proposed by Amin (Amin, 2005). The questionnaires were collected, edited, and the data coded, and that analyzed. Quantitative data were analyzed using SPSS (Garth, 2008), where tables were used based on the data entered in the excel package and a conclusion from the percentages. Then qualitative data were investigated using content analysis, and here findings were compared with quantitative data.

An examination of the quantitative data was performed by using descriptive statistics (frequency and percentages) and statistical tests (Garth, 2008)

3.5 Limitations of the research methodology

However, this research is not without limits. This study uses a cross-sectional design (Maninder, 2016) which means that elements of the research study will be assessed at the current point in time without consideration for the likely future or past influences. The researcher acknowledges that there is limited information available on cybersecurity policy influences in Uganda, which might affect the literature review quality.

Due to the challenge of the timeframe given to conduct the study, the research might not have captured all the necessary information to understand MTN better mobile money services as responses were given for a limited time.

The study also adopts the interview tool for data collection, which is likely to result in respondents with overly stated opinions more willingly presenting them than respondents with less strong opinions and characters.

In addition, even though the respondents were enough to move towards the objectives, the numbers of respondents to the survey were 58, but it could have been better if the survey and interview involved more respondents.

The study also focuses on one telecommunications company in the country out of over four existing telecommunication companies, which is likely to exclude potentially revealing data.

All the information gathered from the data sources mentioned above were reviewed in-depth and extensively analyzed.

2 4. Chapter Four: Findings

This chapter presents the analysis discovered and interprets the study's findings entitled "Assessing the effectiveness of the Amended Uganda Computer Misuse Act in addressing e-commerce cybersecurity risks: A case study of identity theft within MTN Uganda's Mobile Money e-commerce business." In the presentation of findings, tables, frequencies, and percentages were used to explain the results. Quantitative data was analyzed by assessing the consistency of responses obtained from the research instruments. Qualitative data were analyzed by cross-checking sources of information (triangulation), and conclusions were made regarding the obtained findings and the literature review.

4.1 Objective 1: The Quantitative interview

The objective of the quantitative interviews were: to get in touch with users of mobile money; tap into their experience, and; use their experience to design the survey.

Through the 10 interviews conducted, the researcher found that practices around identity theft exist and is experienced in three different ways: Most of the interviewees disclosed the following:

- Discovered that there are some SIM cards registered in their names which do not belong to them.
- 5 Interviewees mentioned that they were called by someone who requested them to send them back mobile money they had mistakenly sent to them, which was not the case.
- The mobile money agent/MTN staff colluded and robbed them of their mobile money.

In addition to the experiences of identity theft, the researcher found that even though they heard of the Act, there is no procedure put in place that ensures the enforcement in the context of knowledge implementation of the Act and cross accountability.

Furthermore, around the enforcement at the MTN level, users' experiences have been that they have to pay in order for penalty procedures to be put in place.

4.2 Objective 2: The Quantitative survey

The objective of the survey was established to determine the current identity theft experiences and techniques within MTN Uganda’s Mobile Money e-services.

The quantitative presentation, analysis and discussion of the research results are organized according to the research objectives. These include findings of that determines the current identity theft experiences and techniques within MTN Uganda’s Mobile Money e-services, as illustrated below.

- **Respondent’s experience with identity theft within the MTN mobile money services**

Results indicated that as many as 70.2% (40) had experienced mobile money identity theft while using the MTN mobile money services compared to 29.8% (17) who did not experience any identity theft with MTN mobile money services.

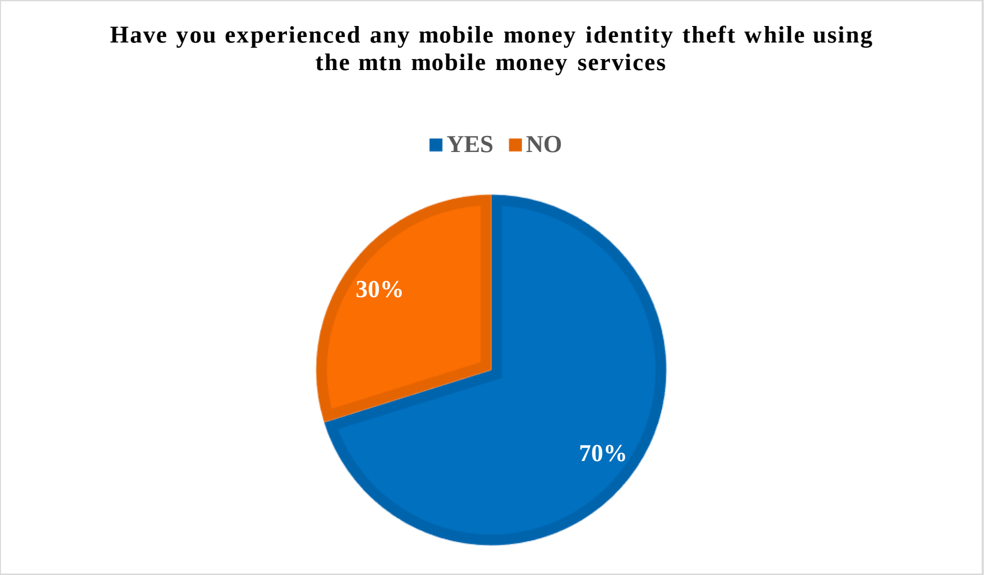

Figure 2: Identity theft experience within MTN mobile money users

Out of the 58 respondents, 34 MTN mobile money services users experienced identity theft at least more than once. 15 reported that they have never experienced any identity theft crimes.

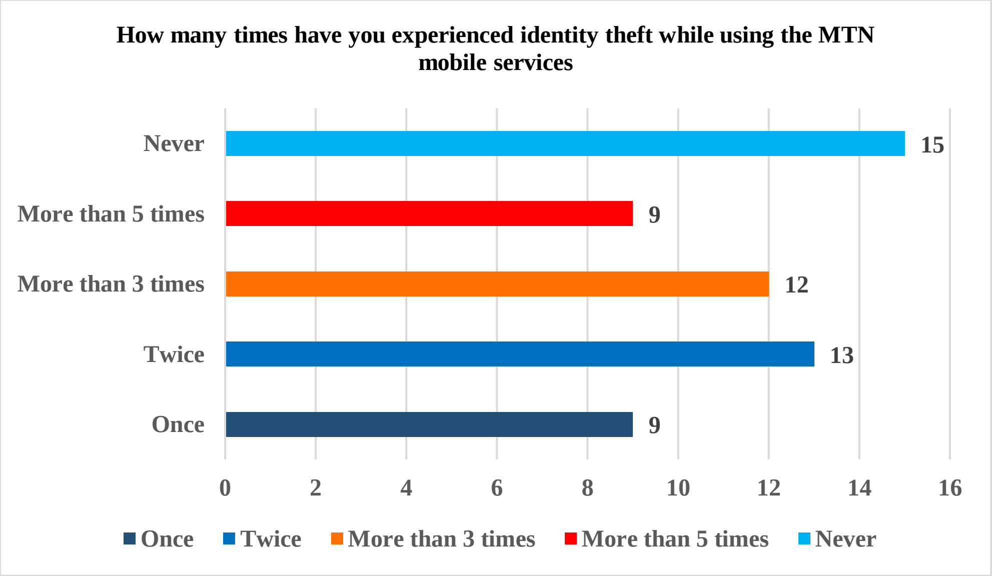

Figure 3: Frequencies that mobile money users experienced Identity theft cybercrime

- **What happened when Identity theft took place while using MTN mobile money services?**

As indicated in figure 4 below, the results show that most respondents (69%) had been called by someone who requested them to send them back the money they had mistakenly sent to them, which was not the case. A few respondents (3%) had the mobile money agent/MTN staff colluded and robbed them of their mobile money. Other identity theft that was reported included when some 14% of respondents found that there were sim cards registered in their names that they did not know, and 1% of respondents were asked to share their mobile money pins. 12% have never experienced any identity theft crimes while using the MTN mobile money services.

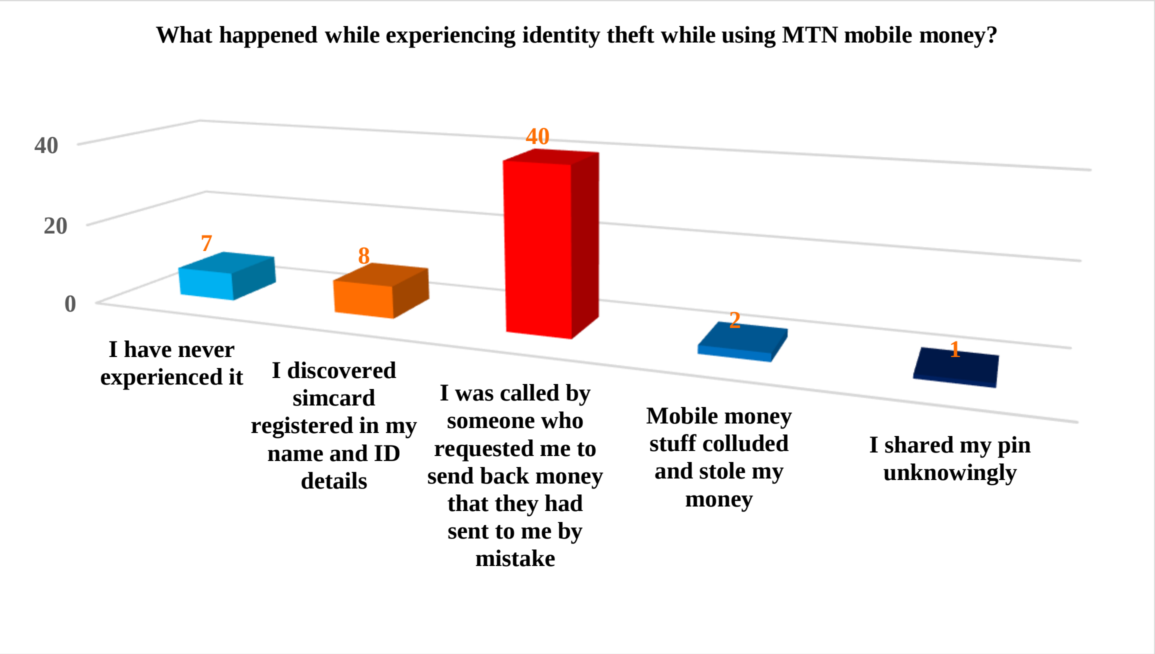

Figure 4: Method experienced in the process of identity theft while using MTN mobile money services.

4.3 Objective 3: Assessment of the Uganda Computer Misuse Act

To assess the effectiveness of the amended Computer Misuse Act in addressing identity theft within MTN Uganda’s mobile money e-services against the findings collected through interviews and the survey.

The current study involved analysis of available data concerning computer misuse in Uganda generally, including identity theft and misuse of Identity information using Uganda's Computer Misuse Act (UCMA) in particular. Numerous scholars reviewed secondary data in the analysis, including official/authoritative sources, including Uganda's Parliament Knowledge Sharing site. The Act was analyzed to determine the effectiveness of Uganda's Computer Misuse Act in addressing cybersecurity risks, in particular, identity theft within MTN Mobile Money e-services. The analysis of the sections of the Act is presented below:

Article 17 of the Act explains “unauthorized disclosure of access code and how a person who commits this offense is penalized”

(1) “A person who knowingly and without authority discloses any password, access code, or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage, or injury to any person or property, commits an offense” (Parilament of Uganda, 2011)

2) "A person who has committed an offense under paragraph 1), upon conviction, may be punished with a fine not exceeding 240 monetary points or a prison term not exceeding 10 years, or both; in the case of subsequent convictions Punishable by a fine of more than 360 monetary points or a prison term not exceeding 15 years, or both” (Parilament of Uganda, 2011).

This section of the Act protects MTN users from the disclosure of their mobile money codes by anyone, which would otherwise lead to the loss of their money.

Article 18 of the Act “explains the unauthorized disclosure of information and how the person who commits this offense is penalized;”

(1) “Except for this Act or for any prosecution for an offense under any written law or following an order of a court, a person who has access to any electronic data, record, book, register, correspondence, information, document, or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access”.

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

This section of the Act addresses the challenge of using information that belongs to MTN mobile money users to register sim cards without their knowledge.

Article 19 of the Act explains electronic fraud and how the person who commits this offense.

(1) “A person who carries out electronic fraud commits an offense and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.”

(2) “For this section, "electronic fraud" means deception, deliberately performed to secure an unfair or unlawful gain where part of communication is sent through a computer network or any other communication.” Another action of the victim of the offense or the step is performed through a computer network or both.”

4.4 Discussion of the results

Objective 1 and 2

The interviews conducted highlights that there is a lot of identity theft that seems to be increasing day but day in Uganda. However, many reported that lack of action might be on the law enforcement and if the penalty mentioned in the Act is actually in force as much as the law indicates it clearly that whoever commits identity theft is liable, punished with a fine not exceeding 240 monetary points or a prison term not exceeding 10 years, or both.

The results were similar to those of Jenny (Jenny, 2019) in her report of GSMA Mobile for Humanitarian Innovation, where respondents in both Bidi Bidi and Kiziba refugee settlements in Uganda and Rwanda that separately pointed out that they had faced fraud problems of providing large sums of money through SMS messages and requesting detailed information on mobile money.

A few respondents (3%) had the mobile money agent/MTN staff colluded and robbed them of their mobile money. Other identity theft that was reported included when some 14% of respondents found that there were sim cards registered in their names which they did not know, and 1% of respondents were asked to share their mobile money pin. The result is consistent with Jenny's (Jenny, 2019), in her report of GSMA Mobile for Humanitarian Innovation wherein Bidi Bidi; respondents reported that mobile money agents sometimes steal information from customers. In addition, participants described the mobile money agent using the customer's PIN and account information to conduct unauthorized transactions on unknown accounts or to transfer all of a person's savings to their account (Jenny, 2019).

Objective 3:

As described in Article 17 Clause 1 and 2, of the amended computer misuse act 2011 (Parilament of Uganda, 2011) explains “unauthorized disclosure of access code and how a person who commits this offense is penalized” The Act applies that MTN users are protected from the disclosure of their mobile money codes by anyone, which would otherwise lead to loss of their money.

A good practice is noted in Article 28 of the cybercrime (prohibition and prevention etc.) (Government of Nigeria, 2015)act 2015 of Nigeria; Any person who knowingly and without authority discloses password access code or any other means of gaining access to any in and computer or network for any unlawful purpose or gain commits an offense” (Government of Nigeria, 2015). “It shall be liable on conviction to imprisonment for a term of not more than two years or to a fine of not more than N5, 000,000.00 or both fine and imprisonment” (Government of Nigeria, 2015).

Article 18 of the Revised Cyber Abuse Act 2011 (Parilament of Uganda, 2011) explains "The unauthorized disclosure of information and how those who commit this crime are punished". This article contradicts the conclusions of the interviewee. It is an access penalty, because this process requires payment, which is why most users finally did not take action in cases of identity theft".

Article 19 of the Act (Parilament of Uganda, 2011)**explains electronic fraud and how to punish those who commit such crimes.**

(1) "Convicted of wire fraud, upon conviction, a fine of not more than 360 points or a prison term of not more than 15 years, or both (Parilament of Uganda, 2011).

(2) "Electronic fraud" in this section refers to deliberate deception for the purpose of illegitimate or illegal profit, in which part of the communication is sent through a computer network or any other communication, and the other party is the victim of the following crime. The sender The act or action is through a computer network or both" (Parilament of Uganda, 2011).

This section is effective in addressing fraud issues however does not explain how it is applicable, how critical it is as it does not indicate any amount of fine for the offenders.

5. Chapter 5: Conclusions, Limitations, and Recommendations

5.1 Conclusion

The impact and cost caused by identity theft are substantial and justify all means being used to control and prevent them. This study has gone towards examining the effectiveness of The Uganda Computer Misuse Act (UCMA), which was enacted in Uganda in 2011 (Parilament of Uganda, 2011) to deal with computer-related offenses, including computer fraud, hacking, spamming, breaches of trust, intellectual property (I.P.) crime, and phishing, among others. The Act was amended in 2017 to adapt to change in technology and the trending sophisticated cybercrimes. This study has shown that despite the amended Act, identity theft is still constantly increasing, and the impact of the Act appears to be somewhat limited due to lack of law enforcement for those liable of the offense.

More than 70% of the respondents of MTN customers had experienced Identity while using the MTN mobile money services. The primary form of identity theft is when most of the respondents are called by someone who requests them to send back the money, and they mistakenly sent it to their mobile money accounts, which was not the case.

Against the definition of the topic as expressed in the description of effectiveness, findings and limitations stated below, the researcher concluded that the amended

Computer Misuse Act of Uganda does not communicate the most use of the Act to combat identity theft within MTN Uganda's mobile money e-services. Further studies should be conducted to raise knowledge on the Act and ensure enforcement nationwide and at the level of MTN.

5.2 Limitations of the research

Several limitations may have influenced the results drawn from this research.

The researcher has not investigated how the Act is enforced at the national level in Uganda. This might require further investigation.

Another limitation is that the research has not investigated how the Act is thoroughly enforced into the MTN; even though it was mentioned, it seemed that the researcher did not have enough knowledge, having spoken to only ten people.

Questions related to a sense of security within services and efforts to raise awareness were limited (questions were only related to experience and techniques used by cybercriminals). It would have been relevant to include inquiries related to security, trust, and awareness campaigns.

Moreover, the researcher does not know to what extend MTN actively promotes the knowledge on identity theft to its users of mobile money.

In addition, the researcher does not know the numbers of prosecutions that have taken place when a criminal is charged with identity theft. It seems that there is a barrier for people to have access. However, even though respondents of the interviews mentioned this, the researcher has not explored this deeply.

Moreover, as in any study that involves surveys, there is a possibility of errors arising from different possible biases, social desirability, indifferences, and random responses. These findings, therefore, need to be considered with caution.

Another limitation is that respondents who do not know about identity theft and cybercrime completed the questionnaire. Due to the small numbers of individuals who have vast knowledge of identity theft and the Ugandan Computer Misuse Act, it was impossible to determine whether those with the knowledge and those without were inclined to provide different answers. Also, it would have been relevant to document if respondents had previous identity thief issues (5 years ago and over). This information would have been significant in assessing the evolution of e-commerce criminal tactics, the Uganda Computer Misuse Act enacted in 1997, and the amended Act in addressing identity theft.

Therefore, an essential contribution to this area of research would be to conduct further effective study with a more redefined research design (longitudinal, experimental studies, etc.)

Finally, in consideration of all mentioned limitations, the researcher thinks that the Act is not effective in addressing identity theft within their mobile services.

5.3 Recommendation

Based on the findings and limitations, the research recommends that in partnership with the relevant government agencies such as the Uganda communications commission, telecommunications companies should continuously sensitize all mobile money users, staff, and agents on the mobile money identity theft mechanisms used by most criminals and prevention measures.

Cybersecurity awareness campaigns should be one implementation in which mobile money users can protect themselves. This awareness includes simple virtual methods for keeping PINs safe and checking their balance before returning money that was allegedly sent to them by mistake. However, as point by (Bada et al., 2015), simple knowledge about good security practices is not enough (Bada et al., 2015, p. 9). Awareness campaigns need to be implemented and other influencing strategies (Bada et al., 2015). This can best be done through training, media events, regular email or text message announcements, system guarantees to prevent PIN leakage, and liaison with law enforcement agencies to investigate and prosecute cases of mobile currency identity theft.

The government should develop appropriate legislation that makes mobile money identity theft preventive and control measures mandatory and ensures their effective implementation by telecommunication companies and other stakeholders.

Significant collaboration is required among all stakeholders to strengthen security and prevent identity theft in the digital e-commerce economy. The private sector often plays a pivotal role in this regard. Across digital markets, MTN and other telecommunication companies act as a vital enabler for change in policies and economic growth. However, private companies, in particular, are also often the most vulnerable to threats and incidents given their limited resources available to direct toward basic security measures within the country.

6 Bibliography

Ali, G. e. (2020). Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda. *Open Access*.

Amin, M. (2005). *ocial Science Research: Conception, Methodology and Analysis.* Kampala: Makerere University Press.

Association of Chartered Certified Accountants. (2019). Africa is leaving itself dangerously exposed to cyber-attacks. *Association of Chartered Certified Accountants*.

Association, I. T. (2020, 08 31). *Uganda - Country Commercial Guide*. Retrieved from International Trade Association-USA: https://www.trade.gov/country-commercial-guides/uganda-ecommerce

Australia Government. . (2020). *Preparing for A Cybersecurity Incidence in Australia.* Australia Government. .

Baganzi et al. (2017). Examining Trust and Risks in Mobile Money acceptance in Uganda. *Sustainability*, 1-22.

Baliño, S. (2021). African Continental Free Trade Area Completes First Month of Trading. *SDG Knowlege Hub*.

Bent, F. (2011). Case Study. *Sage Publications*, 301-316.

Broadcom. (2016). Cyber Crime and Cyber Security Trends in Africa. *Broadcom*.

Brown et al. (2014). Continued Critical Reanalysis. *US National Library of Medine*.

Burnard, P. (1991). A method of analysing interview transcripts in qualitative research. *Longman group UK limited*.

CGAP. (2017). *Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System.* Washington: CGAP publications.

Courchesne, M. (2021). *Establishing a cybersecurity framework for your business.*

Creswell, J. W. (2013). *Qualitative inquiry and research design.* SAGE Publications, Inc.

Deloitte. (2017). Deloitte. (2017). Cyber Risk In Advanced Manufacturing. *Deloitte.* .

Experian 41st Parameter, G. I. (2021). One in six adults has fallen victim to cyber-crime. *Experian 41st Parameter, Gartner, IDC and Bloomberg*.

Forensics Institute Uganda. (2018). Cyber Crime in Uganda. *Forensics Institute Uganda*.

Francis, K. (2018). From 1 July the government will take 1% of your mobile money.

Garth, A. (2008, n.d. n.d). *Analysing data using SPSS.* Retrieved from Sheffield Hallam University: https://students.shu.ac.uk/lits/it/documents/pdf/analysing_data_using_spss.pdf

Global consulting firm Protiviti and North Carolina State University Poole College of Management's Enterprise Risk Management (ERM) Initiative. (2021). EXECUTIVE PERSPECTIVES ON TOP RISKS FOR 2021 AND 2030. *BNP Media*.

Government of Nigeria. (2015). *CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT.* Retrieved from National CIRT Nigeria: https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

GSMA. (2010). *Mobile Money for the unbanked.* GSMA.

Guidance, Ministry of ICT and National. (2019, December 03). *Ministry of ICT and National Guidance*. Retrieved from Ministry of ICT and National: https://ict.go.ug/2019/12/03/the-computer-misuse-act-2011/

Harvey, L. (2004-2020, October 31). *Analytic Quality Glossary*. Retrieved from Quality Research International: https://www.qualityresearchinternational.com/glossary/effectiveness.htm#:~:text=Effectiveness%3A%20A%20measure%20of%20the,do%20for%20a%20specified%20population.

Institute of Chartered Accountants in England and Wales. (2016). The World’s Top Cyber Risks. *Institute of Chartered Accountants in England and Wales*.

Institute, W. P. (2021, 02 10). *Gordon Library*. Retrieved from Gordon Library: https://libguides.wpi.edu/c.php?g=355454&p=2396442

ITU-T X.1205. (2021, n.d. n.d.). *What is Cybersecurity*. Retrieved from International Telecommunication Union: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Jenny, C. (2019). *The digital lives of refugees: How displaced populations use mobile phones and what gets in the way.* GSMA.

KnowBe4. (2020). *The KnowBe4 African Cybersecurity Awareness Report.* KnowBe4.

KPMG. (2021). *Turning cybersecurity risks into business opportunities.* n.p.

Lisa, M. G. (2008). Sem- Strutured Interviews. *The SAGE Encyclopedia of Qualitative Research Methods*.

Little, W. (2016). *Introduction to Sociology – 2nd Canadian Editino.* . BCcampus Open Education.

Maninder, S. S. (2016). Methodology Series Module 3: Cross-sectional Studies. *Indian Journal of Dermatology*, 261-264.

Maria, M. (2014). *The "Effectiveness test" as a tool for law reform.* Maria, M.

Mayring, P. (2004). Qualitative content anaysis. . *A companion to qualitative research*, 159-176.

McAfee. (2020). *McAfee. (2020). How Cybersecurity Policies and Procedures Protect Against Cyberattacks.* McAfee.

Merriam, S. B. (1998). *Qualitative research and case study applications in education.* San Francisco: CA: Jossey-Bass.

Ministry of Justice and Constitutional Affairs. (2014). What is a bill. *Ministry of Justice and Constitutional Affairs*.

MTN Group Management Services . (2019, n.d. n.d.). *MTN Group Management Services* . Retrieved from MTN Group Management Services : https://www.mtn.com/our-story/

Mugoya, D. (2021). *Factors Affecting Consumers ' Adoption of Online shopping in Uganda.* . Kampala: Makerere University.

Nachmias et al. (1987). *Research Methods in the Social Sciences. 3rd Edn., St.* Martin's Press, New York, USA.

Naderifar et al. (2017). Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research. Strides in Development of Medical Education. *Strides in Development of Medical Education*.

Open Access Government. (2020). Africa's Cybersecurity Problems Impact Us All. *Open Access Government*.

OXial. (2020). *Cybersecurity in Africa can emerge stronger from the coronavirus crisis.* Oxial.

Parilament of Uganda. (2011). *The Computer Misuse Act.* Kamapla: Ministry of ICT and National Guidance.

Powers et al. (2010). *Dictionary of nursing theory and research.* Springer publishing company.

Price Waterhouse Coopers. (2021). *Cybersecurity Strategy Report 2021.* Price Waterhouse Coopers.

Saimunur, R. (2014). *Introduction to E-Commerce Technology in Business.* Munich, GRIN Verla.

Serianu,. (2017). Uganda Cybersecurity Report 2017: Demystifying Africa's Cyberscurity Poverty line. *Serianu*, 68.

Slide Share. (2015, 02 13). Retrieved from Slide Share: https://www.slideshare.net/ELIMENG/05-chap-4-research-methodology-and-design1

Sobers, R. (2021). 134 Cybersecurity Statistics and Trends for 2021. *Varonis*.

Stephen, K. (2020). Uganda’s banks have been plunged into chaos by a mobile money fraud hack. *Quartz Africa Weekly Brief*.

The Collaboration on International ICT Policy for East and Southern Africa. (2018). *National Information.* Kampala: Uganda National Information Technology.

The United States Department of Justice. (2020, n.d. n.d.). *What are the identity theft and identity fraud.* Retrieved from The United States Department of Justice: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Thomas, P. (n.d.). *Research Methodolgy and design.* UNISA.

Uganda Communications Commission. (2020). *2019 3rd Quarter Uganda Market Performance Report.* Kampala: Uganda Communications Commission.

UK Parliament. (2021, n.d. n.d.). *What is an Act of Parlaiment*. Retrieved from UK Parlaiment: https://www.parliament.uk/about/how/laws/acts/

United States Homeland Security Science and Technology Division. (2018). Cyber Risk Economics Capability Gaps Research Strategy. *United States Homeland Security Science and Technology Division*.

US Gov. (2021, June 03). *Idnetity Theft*. Retrieved from USA Government: https://www.usa.gov/identity-theft#item-206115

Wilson, R. (2013). *CHARACTERISTICS OF AN EFFECTIVE LAW.* The Law Society of Westtern Australia.

Wisseman, S. (2015-2021). Broken promises: How trust affects cybersecurity. *TechBeacon*.

World Bank. (2020). Global Population Statistics.

World Economic Forum. (2021). *The Global Risks Report 2021.* Geneva: World Economic Forum.

WorldRemit. (n.d, n.d n.d). *WorldRemit*. Retrieved from WorldRemit: https://www.worldremit.com/en/mtn-mobile-money

Yin, R. K. (2014). Case Study Research Design and Methods (5th ed.). *Thousand Oaks, CA: Sage*, 282.

7 Appendices

7.1 Appendix 1: Questionnaire

My name is Grace Acayo, a student pursuing a Bachelor of Business Administration – Major in International Management at the Geneva Business school. I am carrying out a research study to assess the role of Uganda's 2017 Amended Computer Misuse Act in protecting MTN mobile money users from the looming identity theft cybercrime across the country. The data collected through this questionnaire will be handled with the highest levels of confidentiality.

Please note that this is not a test, thus there is no right or wrong answer. Your full cooperation is kindly sought and will be highly appreciated.

Consent form

I agree to participate in the research project titled: **"Assessing the effectiveness of the 2017 Amended Uganda Computer Misuse Act in addressing e-commerce cybersecurity risks: A case study of identity theft within MTN Uganda's Mobile Money e-commerce business"** by the researcher's name Grace Rachael ACAYO

By filling this form, I acknowledge that:

- I have agreed to participate in this study.
- I have been informed of and understand the purpose of this study.
- I understand that I can withdraw from the study at any time without prejudice.
- I understand how the data collected will be used. And that any confidential information will be seen only by the researchers and will not reveal to anyone else.
- Details relating to anonymity and confidentiality have been explained and I understand these.
- I have had the opportunity to ask any questions.
- With full knowledge of all foregoing, I agree, of my own free will, to participate in this study.

SECTION A: IDENTITY THEFT EXPERIENCES AMONG MTN MOBILE MONEY USERS.

This section of the questionnaire is collecting data on the identity theft experiences among MTN **Mobile Money** Users to find out the experiences you've had.

What is identity theft?

Definition: Identity theft may be defined refers to when someone steals your personal information such as your name, address, Social Security Number (SSN), or credit card details, or bank account information to pretend with your Identity in order to commit fraud/steal money or other criminal acts using your data. (US Gov, 2021)

For this study, we are focusing on MTN mobile money users' experiences.

1. Have you experienced any mobile money identity theft while using the MTN mobile money services?

- YES
- NO

2. How many times have you experienced identity theft while using the MTN mobile money services?

- Once
- Twice
- More than 3 times

3. What happened?

A. I discovered that there are some sim cards registered in my name which do not belong to me.

B. I was called by someone who requested me to send them back some mobile money they had mistakenly sent me, which was not the case.

C. The mobile money agent/MTN staff colluded and robbed me of my mobile money

D. Other. Please explain

………………………………………………………………………………………

SECTION B: SOCIO-ECONOMIC AND DEMOGRAPHIC CHARACTERISTICS

This section is collecting data on your socio-demographic characteristics relevant to the research study.

1. What is your Nationality?

A. Ugandan

B. Foreigner

2. What is your occupation?
   - Government official
   - Banking sector
   - Retail sales manager
   - Small Business owner
   - Student
   - Not working
   - Other
3. Are you a user of the MTN Mobile money services?
   - YES
   - NO
4. If yes, how long have you used the MTN Mobile Money for?
   - One month
   - Six months
   - A year
   - More than one year
   - More than 5 years

5. How frequently do you use mobile money services to send money?
   - Once a week
   - Once a month
   - Every month
   - Once a year
   - More than once in a year
   - Never

6. How frequently do you use mobile money services to receive money?

   - Once a week

   - Once a month

   - Every month

   - Once a year

   - More than once in a year

7. Most of my transactions while using the mobile money is for:
    - Transactions connected to my work.
    - Personal transactions (family, friends, etc.)

7.2 Appendix 2: Socio-economic and demographic characteristics of the respondents

Socio-economic and demographic characteristics		Frequency	Percent
	Nationality		
Ugandan		55	95
Foreigner		3	5
	Occupation		
Retails sales manager		3	6
Small business owner		15	26
Health sector		5	10
Finance		11	19
Student		17	29
Others		5	10
	MTN mobile money users		
Yes		57	98
No		1	2
	Duration spent by the respondent while using MTN mobile money services		

One month		1	2
Six month		4	7
A year		6	10
More than one year		21	36
More than five years		26	45
	How frequently respondents used mobile money services to send money		
Once a week		30	53
Once a month		5	8
More than once a month		18	31
Once a year		5	9
	How frequently respondents used mobile money services to receive money		
Once a week		27	47
Once a month		11	19
Every month		15	26
More than once a year		5	8
	Respondents reasons for transactions while using the mobile money		
Transactions connected to my work		19	33
Personal transactions (friends, family, etc.)		39	67

7.3 Appendix 3: Result from Interview

As described by (Burnard, 1991) that there is no one method that can be used for all types of interviews data. This interview was conducted using both open ended and closed ended questions

Speakers	**Transcript**	**Categories**
First interviewee	**human resource manager, Ugandan**	**Nationality and occupation**
	Yes, it's a widely used networking vendor.	Do you use MTN
	But sometimes you get phone calls from hackers who have sent text messages with money. Money, saying the money has entered your account, and you should sell it back to them when the company is actually not very strict the forwarded message.	When asked if they have experienced any Identity theft while using MTN mobile money services
	nothing you don't go through with the message or you just delete. Okay, you have to check your account balance and make sure it's	When asked what they did after this experience
	They did not do anything.	How MTN tried to solve the problem
	introduce the nationwide really discussion for everyone whereby you have tore register your SIM card, your national I.D. They stop issuing old I.D.s, without an in SIM cards that are not registered under someone else's name.	Advice recommended
Second interviewee	**I work as an accountant. Ugandan**	**Nationality and occupation**
	Oh it's been 20 years now	Do you use MTN
	From the top of my head I think it has been three occasions. I had my phone. And the money disappeared from my phone.	When asked if they have experienced any Identity theft while using MTN mobile money services

	I just, I really don't know. And I found my money was withdrawn from my phone.	
	And when they tried to fill out for the police. Okay, they found a number. But the number was really disconnected and not assigned to anyone. We tried to call back number But the number was really disconnected and not assigned to anyone.	When asked what they did after this experience
	No, but then when it came to the monetary reimburse my money.	How MTN tried to solve the problem
		Advice recommended
Third interviewee	**Pastor, Ugandan**	**Nationality and occupation**
	Yes, I am a user from MTN mobile.	Do you use MTN
	Yeah, I think I can see maybe on the threats. The kind of people that tired to call me.	When asked if they have experienced any Identity theft while using MTN mobile money services
	That is another thing I don't know how they get my numbers but they only call me and they just strip away they even call me by my name. Yeah. Okay, with the mobile with the MTN Uganda, if you, you know, if you're kind of like trying to send the money to the member. He will show you the name of the project. So, that's how they do it.	How did they get your number
	I wish they could make it normal for everybody. Because some people you have different categories of rich and the middle, kind of like they're so Python is very common to kind of like get	When asked what they did after this experience

	money to try, you know, confusing. And then you get your people killed, and then you try to go and find out who did it using the numbers went in and they will. You will have to pay. And the least you can pay the 5000 is and that is at least because I tried that, and they told me that.	
	Not on my side, at least at the time I've been tried, you know, they tried to call me. You know the pm center and Gen center and kinda like when they tell me they have one single name whenever they get to we get that point that we do want something, it's so many different units that the individual names.	How MTN tried to solve the problem
	eah, that was a bit mad attorney because they should have been doing the right thing but, you know, getting your system in to use, but they're not implemented and I believe they have the Cybercrime knowledge and ml they're not just sitting passively now. That may take that may be the good, the good. they don't know how to implement the law, maybe	Advice recommended
	Yeah, it baffles me. Because when it comes to tracking like somebody did. Maybe killed a passion through, you know, using the same line of the NBN, there's all this capital. If you have the money to pay them, and they will track you, you know, and they will get the signals, but I just wonder why they	

	can't use the same system, to get this dude's mobile money. I don't know I don't know why they're not using that because we have testimonies that people have been killed, and the kid has arrested because MTN used to get them to I guess.	
Fourth interviewee	**Ugandan, not working**	**Nationality and occupation**
	YES	Do you use MTN
	Oh, someone called. And I put on my, my thing, but I understood that they are con men, as reported to MTM. So, they, they have never heard my man.	When asked if they have experienced any Identity theft while using MTN mobile money services
		How did they get your number
	I called MTN	When asked what they did after this experience
	Yes, they called call the person, as soon as I called and they found the person. Yes, they did found that person and lost his number.	How MTN tried to solve the problem
		Advice recommended
Fifth interviewee	Ugandan, NGO	**Nationality and occupation**
	Yes, I have been using the network for a while now	Do you use MTN
	Several times but since I know their tricks, I just switch off the phone	When asked if they have experienced any Identity theft while using MTN mobile money services
	I have no idea but I think it's a network of criminals who do business with MTN employees to get our information. It's a large gang of thefts and that is their job	How did they get your number
	I did not do anything because I know they system, they don't help. So I just checked to make sure that	When asked what they did after this experience

	my money and passwords are all changed	
	MTN don’t really care, they say its your fault or you pay them to search for the person	How MTN tried to solve the problem
Sixth interviewee	**Master Student, Ugandan**	**Nationality and occupation**
	I have used the MTN for a long time now and been using the mobile money for over 10 years now	Do you use MTN
	These mobile money thieveshave been in the game for quite sometime..but they are just like any other scammers out there. I have been called several times that I won some money, and it was sent to my account and I should check. But before I did I asked how I won the money but the person went off because I was asking too many questions. So I ended up not blocking the number and not opening my mobile account for that day to avoid any risk	When asked if they have experienced any Identity theft while using MTN mobile money services
	I have no idea	How did they get your number
	I just blocked the number because we know that nothing will be done	When asked what they did after this experience
	Not at all as I did not actually inform them	How MTN tried to solve the problem
Seventh interviewee	**Filed/NGO, Ugandan**	**Nationality and occupation**
	Yes, I have used it for awhile now and its network coverage is good even in the rural areas	Do you use MTN
	Yes, on several occasions. I get calls from unknown people trying to con me.	When asked if they have experienced any Identity theft while using MTN

	They use lines like you have won a price.	mobile money services
	I don't really know	How did they get your number
	Not really much you can do about it other than block the number.	When asked what they did after this experience
	Reporting to MTN is a waste of time.	How MTN tried to solve the problem
Eighth interviewee	**Small Business owner, Ugandan**	**Nationality and occupation**
	Yes but not often. I find their services quite expensive	Do you use MTN
	No, I have not experienced that.	When asked if they have experienced any Identity theft while using MTN mobile money services
	Not applicable I guess	How did they get your number
		When asked what they did after this experience
		How MTN tried to solve the problem
Nineth interviewee	**Small Business owner, Ugandan**	**Nationality and occupation**
	Yes, for most of my transactions. I own a MTN mobile money business.	Do you use MTN
	Yes, given the nature of the business, I get that a lot. Some come with fake shillings to make deposits	When asked if they have experienced any Identity theft while using MTN mobile money services
	Sometimes the MTN employees connive and carry out such theft	How did they get your number
	Report to the police but nothing is usually done	When asked what they did after this experience
	I didn't report to MTN.	How MTN tried to solve the problem
Tenth interviewee	**Government, Ugandan**	**Nationality and occupation**
	Yes, I use it as a second option.	Do you use MTN
	Aside from calls from scammers to lure me into	When asked if they have experienced any Identity

	sending money, I haven’t really experienced serious theft .	theft while using MTN mobile money services
	I can’t tell	How did they get your number
	I report those numbers to MTN	When asked what they did after this experience
	They blocked those random numbers	How MTN tried to solve the problem