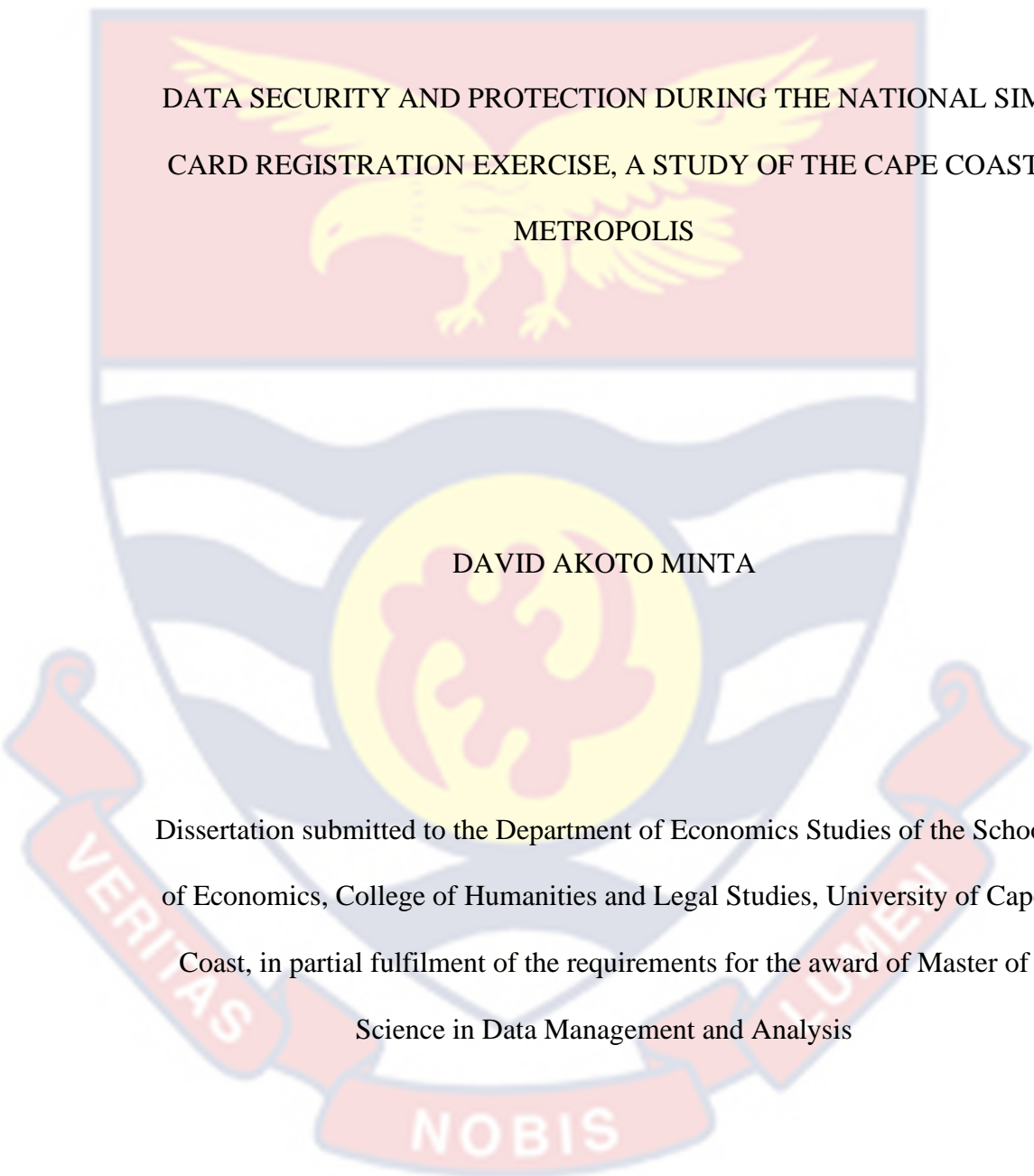


UNIVERSITY OF CAPE COAST



DATA SECURITY AND PROTECTION DURING THE NATIONAL SIM
CARD REGISTRATION EXERCISE, A STUDY OF THE CAPE COAST
METROPOLIS

DAVID AKOTO MINTA

Dissertation submitted to the Department of Economics Studies of the School
of Economics, College of Humanities and Legal Studies, University of Cape
Coast, in partial fulfilment of the requirements for the award of Master of
Science in Data Management and Analysis

OCTOBER 2022

DECLARATION

Candidate's Declaration

I hereby declare that this dissertation is the result of my own original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature: Date:

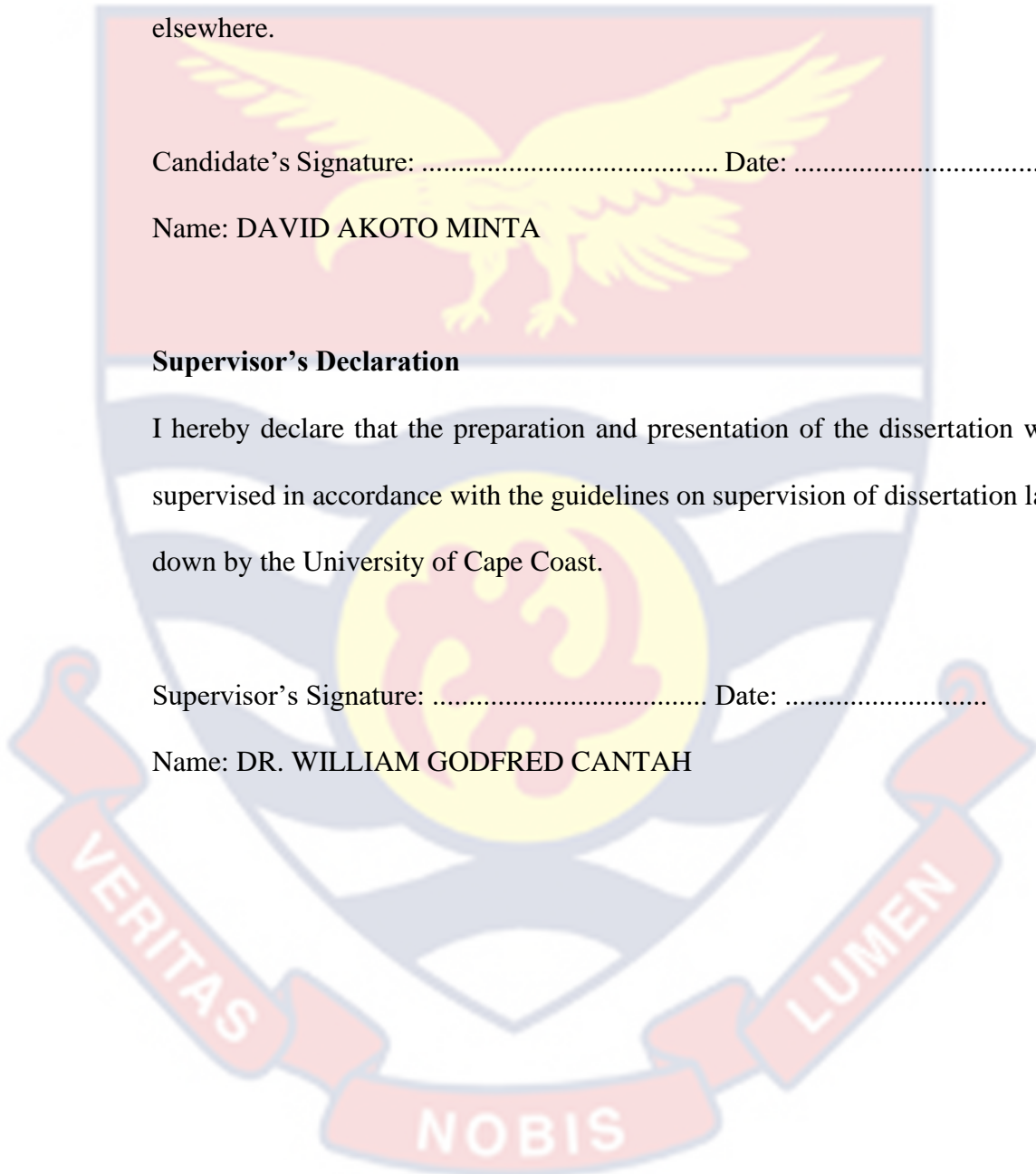
Name: DAVID AKOTO MINTA

Supervisor's Declaration

I hereby declare that the preparation and presentation of the dissertation was supervised in accordance with the guidelines on supervision of dissertation laid down by the University of Cape Coast.

Supervisor's Signature: Date:

Name: DR. WILLIAM GODFRED CANTAH



ABSTRACT

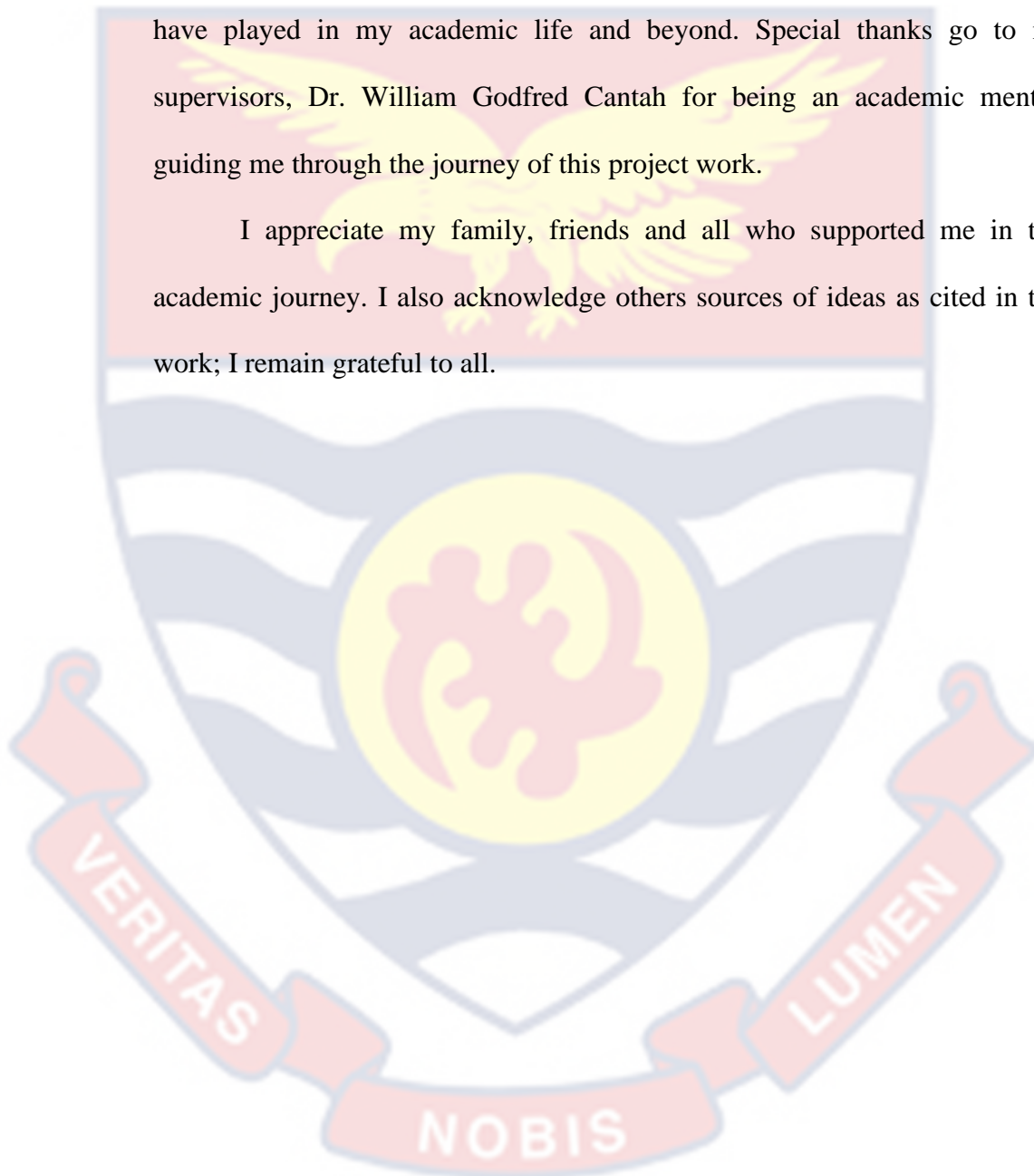
This study sought to investigate data security and protection during the national SIM card registration exercise within the Cape Coast Metropolis in Ghana. The theory underpinning the study was the protection motivation theory. The study employed the multi-case study approach under the qualitative method. Data was collected from nine participants; 3 network provider officials and 6 SIM registration subscribers with an open-ended questionnaire and also from additional secondary sources. The data was analyzed using thematic and content analysis. The study found that the processes that the respondents narrated were largely consistent with the laid down SIM registration procedures, respondents had divergent concerns about data safety and security and it was also realized that the National Information Technology Agency (NITA) is responsible for storing and securing user data. The study recommends that the government and respective agencies involved in the SIM registration process do well to educate the public on the importance of the SIM registration exercise to ensure maximum cooperation and also launch a mobile application for which SIM registration can be completed in the comfort of user's homes without any human interface to ensure maximum data privacy and security.

ACKNOWLEDGEMENT

I am grateful to the Almighty God for granting me the life and strength to complete this project work and my degree programme.

I appreciate the role that the lecturers of the University of Cape Coast have played in my academic life and beyond. Special thanks go to my supervisors, Dr. William Godfred Cantah for being an academic mentor; guiding me through the journey of this project work.

I appreciate my family, friends and all who supported me in this academic journey. I also acknowledge others sources of ideas as cited in this work; I remain grateful to all.



DEDICATION

To my wife Mrs. J. O. A. Minta, and my three kids.



TABLE OF CONTENTS

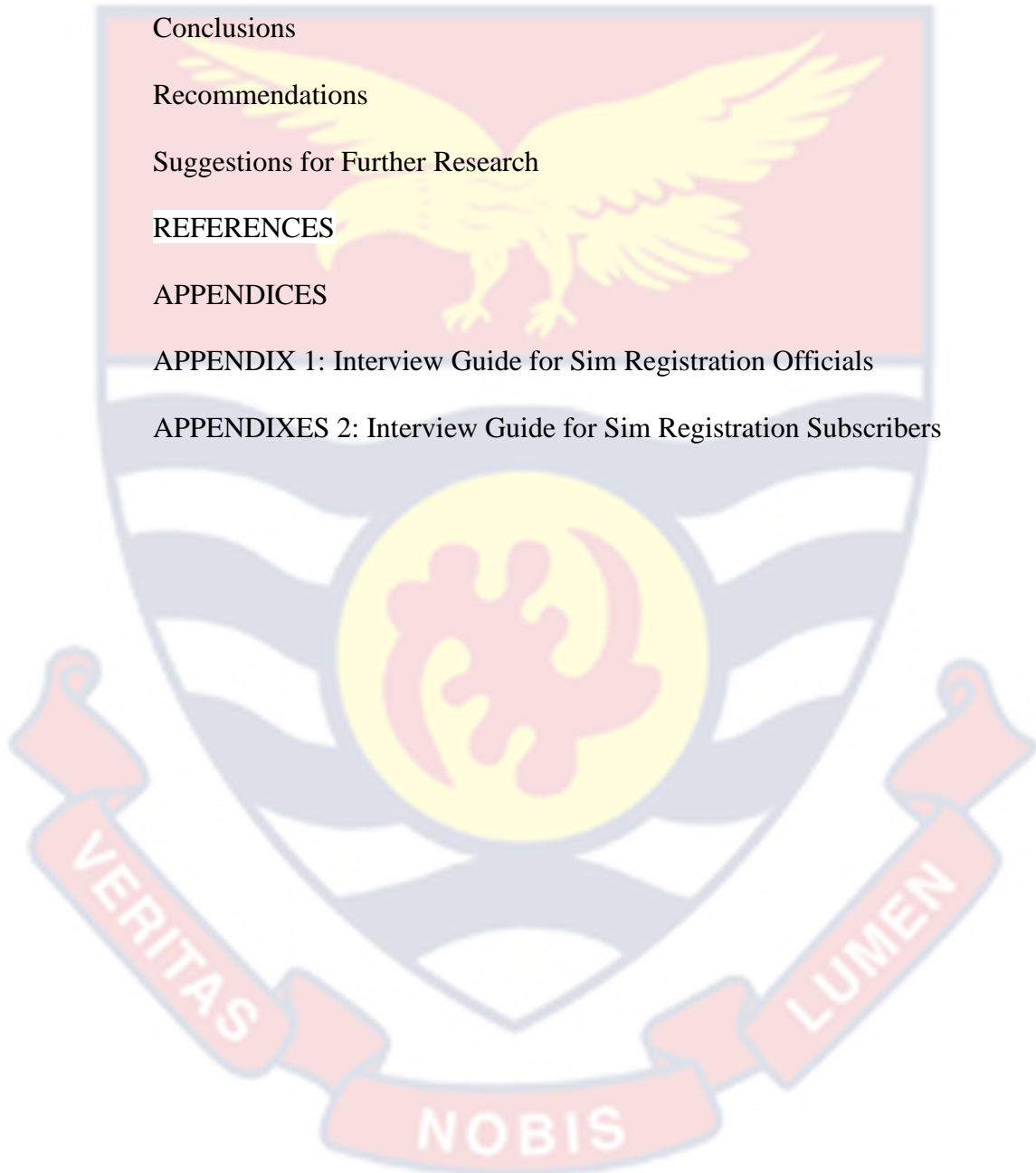
Content	Page
DECLARATION	ii
ABSTRACT	iii
ACKNOWLEDGEMENT	iv
DEDICATION	v
TABLE OF CONTENTS	vi
LIST OF TABLES	x
LIST OF ABBREVIATIONS	xi
CHAPTER ONE: INTRODUCTION	
Introduction	1
Background to the Study	1
Statement of the Problem	4
Purpose of the Study	6
Research Objectives	6
Research Questions	7
Significance of the Study	7
Delimitations of the Study	7
Organization of the Study	8
CHAPTER TWO: LITERATURE REVIEW	
Introduction	9
Theoretical Review	9
Protection Motivation Theory	9
Conceptual Review	12
Information	12

The Concept of Data Privacy	12
Data Governance Laws	13
Fair Information Practices	14
The Concept of Data Security and Protection	15
Types of Data Security	16
Encryption	16
Data Erasure	17
Data Masking	17
Data Resiliency	17
The Concept of Data Integrity	17
Data Security and Protection in Ghana	19
Factors That Can Undermine the Security and Protection of Data	21
Ways of Improving Security and Protection of Data during SIM	
Registration Exercise	22
Empirical Review	24
Chapter Summary	26
CHAPTER THREE: RESEARCH METHODS	
Introduction	27
Research Philosophy/ Paradigm	27
Research Approach	28
Study Area	31
Population	32
Sample and Sampling Procedure	33
Sample Size Selection	34
Data Collection Instrument	35

Reliability and Validity of Data and Research	36
Data Collection Procedure	37
Data Processing and Analysis	37
Ethical Considerations	38
Chapter Summary	39
CHAPTER FOUR: RESULTS AND DISCUSSION	
Introduction	40
Objective One	40
Purpose of the SIM Re-registration	41
Basic Requirements and Information Needed for SIM Registration	44
The SIM Registration Process	46
Stage One	48
Stage Two – Bio Capture	49
Objective Two	50
Initiator of the SIM Registration Exercise	50
Legislations	52
Regulations	54
Guidelines and Codes	55
Personnel and Institutions Involved in the SIM Registration Exercise	56
Storage and Ownership of Data	61
Objective Three	63
Safety Concerns of Data	63
Factors That Could Compromise the Security and Protection of Data	65
Chapter Summary	67

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND
RECOMMENDATIONS

Introduction	68
Summary	68
Conclusions	71
Recommendations	71
Suggestions for Further Research	72
REFERENCES	73
APPENDICES	79
APPENDIX 1: Interview Guide for Sim Registration Officials	79
APPENDIXES 2: Interview Guide for Sim Registration Subscribers	82



LIST OF TABLES

Table		Page
1	Total number of respondents	34



LIST OF ABBREVIATIONS

CCMA	Cape Coast Metropolitan Assembly
ECOWAS	Economic Community of West African States
GIFEC	Ghana Investment Funds for Electronic Communication
GoG	Government of Ghana
GP	Ghana Post
GSMA	Global System for Mobile Association
MNO	Mobile Network Operator
MoCD	Ministry of Communications and Digitization
NCA	National Communications Authority
NIA	National Identification Authority
NITA	National Information Technology Agency
OECD	Organization for Economic Corporation and Development
PMT	Protection Motivation Theory
SIM	Subscriber Identification Module
SRA	Secure Remote Access

CHAPTER ONE

INTRODUCTION

Introduction

Biometric SIM card registration has grown into a worldwide technique for enhancing the security and verification of the identity of individuals. On October 1, 2021, the Government of Ghana (GoG), through the Ministry of Communications and Digitalization (MoCD), commenced the Subscriber Identity Module (SIM) card re-registration exercise all over the country using the Ghana Card. This study sought to examine the situation of data security and protection during the SIM card reregistration exercise in the Cape Coast Metropolis. This introductory chapter discusses the background to the study, the significance of the study, the research questions and generally, the organization of the entire study.

Background to the Study

Privacy liberty is an innate human right that cannot be taken away or incorporated into any law or policy enacted or proposed by the government (Izuogu, 2010). In 1999, just 10% of the population in Africa was within range of a mobile signal; by 2009, that percentage had increased to 60%. (Aker and Mbiti, 2010). Africa is home to more than one billion people at present.

The adoption of electronic forms of identification has grown in popularity due to their accessibility, low cost, and flexibility compared to older traditional methods. However, approximately 500 million people across Africa are undocumented and lack official identification, such as birth certificates or national IDs (Van der Spuy, Bhandari, Trikanad & Paul, 2021).

The process of re-registering Subscriber Identity Module (SIM) cards with the Ghana Card was initiated across the entire nation on October 1, 2021, by the Ministry of Communications and Digitalization (MoCD) on behalf of the Government of Ghana (GoG). The activity, scheduled to last for one year and one month, will be completed by November 30, 2022. Throughout this exercise, the details on an individual's Ghana Card, a national identification card, will be synchronised with those used for the SIM authorization to establish a centralized database. This database will be housed in a Central SIM Registry at the National Information Technology Agency (NITA), which has a non-accessible policy.

According to the report published by the Global System for Mobile Communications (GSMA) in 2016, pre-paid SIM card registration requirements are compulsory in many countries, and customers must provide identification documentation to activate and make use of a mobile SIM card. According to John (2019), this policy is adopted by many countries to assist alleviate safety issues and manage illegal and anti-social conduct.

Because of the relative anonymity of its users, criminals often take advantage of the fact that unlicensed or improperly registered SIM cards can be used as conduits. Pakistan was one of the first countries to implement obligatory biometric SIM card registrations to solve this problem. Because pre-activated SIM cards were utilised in criminal activities like terrorist plotting, the new method was developed as a restrictive step to stop their sale (Beatrice, 2020). According to Bischoff (2020), numerous nations now have biometric registration and accompanying regulations. These countries include Afghanistan, Bahrain, Bangladesh, Benin, China, Nigeria, Oman, Pakistan,

Peru, Saudi Arabia, Singapore, Tajikistan, Thailand, Uganda, Rwanda, United Arab Emirates, and Venezuela.

Rwanda was also among the first East African nations to adopt Biometric SIM card registration, passing Regulation N°004/R/ICT/RURA/2018 of 26/04/2018 controlling the SIM card Registration in Rwanda. The Law was enacted by Government Gazette No.31 of 30/07/2018 (Beatrice, 2020).

Data acquired from registered SIM cards is immediately connected to a subscriber's national identity card database. This ensures that there will be no more instances of incorrect information or document fraud because nobody can forge biometrics. In essence, for financial institutions, telecommunications, and other companies dependent on some degree of confidence in the consumers they serve, biometric identification is increasingly employed as a "Know Your Customer" device to deter fraudsters from the client base. This is notably the situation in recent years. A biometric search gives an operator of service the capability to determine whether or not a candidate is actually who he claims to be and whether or not he is making any effort to hide his true identity.

The National Communications Authority (NCA) of Ghana posited that the need for SIM registration includes, to:

- a. Keep your SIM card safe and always connected
- b. Design and construct an honest SIM database, which will increase users' faith in and sense of safety about using services that rely on the communication system.
- c. Discourage fraudulent and illicit activity
- d. and secure business transactions using SIM cards

- e. assist in determining, at any given time, the precise number of active and correct SIMs currently on the networks.

Other reasons are that operators can use the results to categorise their clientele better and tailor future offerings to their most valuable segments by performing this process. Additionally, the Regulator, NCA, will use the statistics derived from the data to enforce stricter rules on the business. Also, by allowing citizens to use E-Government services and other private e-services, SIM Registration would boost economic growth and eventually legalize the informal economy. Finally, SIM Registration will also aid in promoting financial inclusion for the most marginalized populations.

It is these reasons that have necessitated the SIM registration action in Ghana.

Statement of the Problem

The attempt to re-register 42,749,662 SIM cards across Ghana with limited registration centres and within thirteen months by the MoCD tends to cause breaches in data security and protection during the exercise.

On the issue of data storage, security and protection, MoCD has explained that:

1. Firstly, following the Data Protection Act of 2012, all of this information will be kept in a centralised SIM register at the National Information Technology Agency (NITA) with restricted access (Act 843)
2. In the event of a crisis or national security threat such as a terrorist attack, natural disaster, or public health issue, law enforcement authorities will be able to access the data upon issuance of a court order

to help prevent, identify, investigate, and prosecute fraud and other illegal activity.

3. The Data Protection Commission is a significant participant in this activity.

Anecdotal evidence and national news publications show that the following factors of the registration exercise may compromise the security and protection of citizen's data:

1. the limited period for the practice resulting in overcrowding and stampede at little registration centres,
2. the inconsistent processes of data collection across different telecommunication company registration centres, and
3. the increasing "human factor" in the data collection due to the need for more registration avenues.

People waiting in long queues at various telecommunications offices and centres hoping to reregister their SIM cards have been an increasingly regular sight in recent years. "Some subscribers say they had to go to the reregistration venues as early as 3:00 am while others had to return to the venue on a second day as they could not be served the previous day, adding that it was stressful going through the exercise", according to a Ghanaian Times online publication on January 7, 2022. It is also observed that to reduce the congestion at their service centres, most mobile telephony companies have devised other ways of increasing registration centres, hence the increase in the "human factor" further compromising data security and protection. For example, MTN Ghana, a mobile telephony company, issued an official public statement on Wednesday, January 5, 2022, directing subscribers to visit its branch offices, connect stores,

distributor branch offices, light retail stores (volume management facilities), retail centres, and agent touch points throughout the country to be served to decrease the overcrowding at service centres, as reported by the Ghanaian Times.

From the researcher's survey and review of extant literature, there has not been any study of data security and protection in a mass and limited SIM registration exercise of such nature as in Ghana. Thus, presenting an additional research gap is what necessitates this study. Against this background, the researcher undertakes this study to ascertain whether there is enough protection and security for the exchange of data at SIM registration centres within the Cape Coast Metropolis.

Purpose of the Study

This research aims to assess the mechanisms put in place to guarantee data security and protection during the national SIM card registration activity in the Cape Coast Metropolis, Ghana.

Research Objectives

The specific objectives of the study are to:

1. Identify the processes that are involved in the data collection and synchronization exercise;
2. ascertain the persons and institutions that are involved (directly and indirectly) in the data collection and synchronization exercise at all levels;
3. find out the factors that could compromise the security and protection of data.

Research Questions

In summary, there is a need for a better understanding of the processes and people involved in the data collection and synchronization to identify the factors that could compromise the security and protection of data collected during the SIM card re-registration exercise. More specifically, the following research questions need to be addressed.

1. What are the processes involved in the data collection and synchronization exercise?
2. Which persons and institutions are involved (directly and indirectly) in the data collection and synchronization exercise at all levels?
3. What are the factors that could compromise the security and protection of data?

Significance of the Study

This study of the SIM card re-registration exercise seeks to improve data security and protection ultimately. It is vital to whip up the confidence of the citizenry to willingly and fully participate in the initiative. The study findings will also stimulate the government of Ghana through MoCD to tighten its data security and protection policies at the data entry level. Researchers can also use the findings and recommendations of this study as the basis for pursuing other related studies for economic development and academic purpose.

Delimitations of the Study

The study is limited to only the Cape Coast Metropolis in the Central Region of Ghana. Three registration centres are used for the analysis: the MTN, Vodafone and AirtelTigo main offices in Cape Coast. Variables like

employment status, marital status and level of education are not included in this study as it does not affect the study's objectives.

Because this study was conducted using a qualitative method, the findings may be different if conducted using a quantitative or mixed methodology. Certain authorities were reluctant to share critical data that would have strengthened the findings report. The constraints of time and money were also a limiting factor.

Organization of the Study

This research is organized into five essential chapters. The introductory chapter goes into the study's background, the problem that prompted it, its goals, research targets and questions, its relevance, and its bounds and restrictions. The second chapter assesses the theoretical, conceptual, and empirical literature that underlies the research. The third chapter discusses the research methodologies, including the methodology and data sources, in addition to the data collection and analysis processes. The fourth chapter presents the study's results and discusses its findings. Lastly, the fifth chapter summarizes the investigation and conclusion and provides suggestions for the research.

CHAPTER TWO

LITERATURE REVIEW

Introduction

An overview, a summary, and an analysis (or criticism) of the present state of knowledge of international and local data security and protection principles and practices are presented in the literature review. It also contains a review of methodological concerns and recommendations for further investigation (Taylor, 2007).

Theoretical Review

The theoretical literature review helps to determine what theories previously existed, the links between those ideas, and the extent to which the theoretical concepts have been studied, and it also helps build new hypotheses that may be investigated. A solid theoretical framework gives the study a sense of direction and helps explain and generalize findings. Given the nature of the study, the author found a critical theory that relates to this study: the Protection Motivation Theory, which is discussed in-depth in the subsequent paragraphs and shows how it is relevant to the topic of study.

Protection Motivation Theory

Rogers (1975) established the protection motive theory (PMT) as a theoretical framework with the purpose of comprehending the effect that fear appeals have. In Rogers' (1983) revision of the PMT, the theory was enlarged to offer a wider description of the power of persuasive messages, with an emphasis on the cognitive capacities that allow change in behavior. It was created to explain how individuals are prompted to behave in a self-protective way towards a perceived health danger. The purpose of its creation was to create

a better grasp of the notion. It was primarily intended for use in the field of disease prevention and health promotion, and it explains why and how people take preventative measures when they feel threatened. It consists of four main parts: the first "threat appraisal," accompanied by "coping appraisal," which includes "response efficacy" (the perception that specific procedures will lessen the threat), and "self-efficacy" (the individual's notion of their capacity to take the necessary steps to reduce the threat) (Westcott, Ronan, Bambrick & Taylor, 2017). The Protection Motivation Theory is applicable to "any threat for which there is an efficient recommended reaction that can be followed by the individual." (Floyd, Prentice-Dunn & Rogers, 2000).

Following that, study of PMT has generally been undertaken in one of two ways: first, PMT has been utilized as a framework to create and analyse persuasive messages; second, PMT has been used as a social cognitive model to anticipate health - associated actions. It was the initial study on the persuasive power of fear appeals that highlighted the contexts in which fear appeals may affect attitudes and behaviors that established the framework for the creation of PMT. One of the most important questions that needed to be answered was whether or not fear appeals can directly influence people's views and behaviour, or whether or not their effects are more indirect (Norman, Boer, Sevdal & Mulllan, 2015).

Rogers (1975) came up with the PMT in order to bring more clarification to the field of study on fear appeals. Specifically, Rogers (1975) tried to identify the significant variables in fear appeals in addition to their cognitive mediating role consequences. This was done in an effort to better understand how fear appeals work. The work of Hovland, Janis, and Kelley (1953), who

hypothesised that there are three primary stimulus factors at play in a terror appeal, served as the foundation for the development of PMT.

the degree of noxiousness or intensity of an incident, the probability that the incident will take place if no preventative measures are taken or if existing preventative measures are not altered, and the viability of a suggested method of dealing with a negative experience in terms of its ability to mitigate or get rid of the problem.

Rogers (1975) incorporated these factors in the first construction of PMT and also claimed that each sensory variable triggers a matching cognitive mediational mechanism. He did this in order to test his hypothesis that PMT is a general model applicable to a wide range of situations. Therefore, the amplitude of the noxiousness of an incident is the initial factor in initiating perceptions of the event's intensity, the probability that they will take place is the initial factor in initiating perceptions of vulnerability, and the provision of an effective coping response is the initial factor in initiating perceptions of the response's efficacy. That is to say, the influence of the stimulus elements in a fear appeal is modulated not only by perceived severity, but also by perceived vulnerability and perceived efficacy of a response. These impressions, in turn, influence individuals' motivation to defend themselves (i.e., intention to follow the behavioural advice). Protection motive is considered to be the proximal determining factor of protective behaviour due to the fact that it "arouses, maintains, and directs action" (Rogers 1975).

The goal of PMT is to identify the threat, evaluate it, and then counter it with practical and efficient mitigation measures (Westcott et al, 2017). The fear of losing data that always been the plight of data collectors since most of this data contains important details for key decision making and the loss of it may cause great havoc. Protection Motivation Theory comes to play as it seeks to recognise and mitigate this danger.

Conceptual Review

The conceptual review discusses the main concepts and themes relating to the study.

Information

Information is defined as the disparity between the recipient's prior and post-informational level of knowing (Bell, 1957, p. 7).

The terms "information" can be used in three different ways: as a process, as knowledge, and as a physical object. The process of receiving knowledge such as news is known as information. Knowledge is what's being conveyed through information-as-process, so the two go hand in hand. The intangibility of information as knowledge makes it unique. It is intangible and impossible to quantify or directly touch. Data and written materials are examples of "information as thing," which includes intelligible physical items (Buckland, 1991).

The Concept of Data Privacy

Data privacy refers to the safeguarding of personally identifiable information from persons who have no right to view it and the provision of individuals with the power to control who has access to their own private information. This personally identifiable information could involve a person's

name, setting, additional contact details, or behaviors either online or in the real world. There are numerous jurisdictions that see privacy as a fundamental human right, and as a result, there are laws in place to protect individuals' personal information. Data privacy is particularly crucial because in order for people to feel comfortable engaging in activities online, they need to have faith that their data will be managed with care by the relevant parties.

If users' personal identifiable information is not protected or they have no say in how it is utilized, it can be exploited in a number of ways: criminals can use it to swindle or harass them, and companies can sell it to marketers and other third parties without their knowledge or permission, leading to unsolicited communications from those companies. Any one of these consequences can have a negative impact on an individual. These actions can lead to fines, sanctions, and other legal implications for an organization, in addition to causing irreparable harm to the reputation of the business (Cloudflare, 2022).

Data Governance Laws

As a consequence of the enhancements in data collection and surveillance capabilities generated by advancements in technology, governments all over the globe are starting to pass laws that supervise the kinds of data that can be collected about clients, how that data can be used and how data must be sequestered and safeguarded. The following constitute a few of the most key legislative privacy frameworks that you should be aware of:

- The General Data Protection Regulation (GDPR) establishes standards for the collection, storage, and processing of personally identifiable information about persons inside the European Union (EU) and grants

individuals' certain rights with respect to this information (including a right to be forgotten).

- Canada, Japan, Australia, Singapore, and other nations have enacted national data protection laws to ensure the privacy of their citizens' personal information. The Data Protection Act of the United Kingdom and the General Law of Brazil on the Protection of Personal Data are two examples of laws that are quite comparable to the General Data Protection Regulation.
- The Data Protection Act, 2012 (Act 843) is the primary piece of national legislation governing data protection in Ghana. It addresses how the personal information of citizens is to be utilized and administered by the government.

Fair Information Practices

A significant number of the data protection legislation that are currently in effect are founded on fundamental privacy concepts and practises, such as those that are outlined in the Fair Information Practices Act. The term "fair information practises" relates to a set of standards that regulate the gathering and exploitation of data. In 1973, a group functioning as an advisor to the United States Department of Health, Education, and Welfare came up with the original recommendation for these guidelines. In subsequent years, the international Organization for Economic Cooperation and Development (OECD) incorporated them in its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as a requirement that ought to be committed to.

The Fair Information Practices are:

- *Collection limitation: There ought to be restrictions on the amount of private information that can be gathered.*
- *Data quality: When collecting personal information, care should be taken to ensure that it is reliable and pertinent to the intended use of the data.*
- *Purpose specification: The utilization of personally identifiable information needs to be clarified.*
- *Use limitation: It is inappropriate to use data for any reasons other than those that were specified.*
- *Security safeguards: Data should be kept secure*
- *Openness: Individuals have a right to know how their personal information is collected and used.*
- *Individual participation: People have the right to request access to their personal information, receive a copy of that information, understand the reasoning behind any denial of access, and have inaccurate or deleted information rectified or removed.*
- *Accountability: Everyone involved in the data collection process ought to be held accountable for adhering to these guidelines.*

The Concept of Data Security and Protection

The technique of protecting digital information over its complete life cycle in order to prevent it from being damaged, stolen, or accessed in an unauthorized way is referred to as data security. It comprises everything, including software, hardware, storage media, and user devices, as well as access and operating methods, as well as the rules and procedures of corporations.

Tools and technologies are applied in data security to increase the transparency of an organization's data and how it is being utilized. Data may be safeguarded utilizing these approaches through processes such as concealing data, encryption, and the obliteration of sensitive information. The technique also supports organizations in simplifying their audit strategy and adhere to increasingly severe rules surrounding the protection of personal data.

Types of Data Security

A diverse assortment of data security methods can be used within an organisation in order to protect its users, devices, networks, and other components of its infrastructure. The following is a list of some of the most prevalent types of data security that companies should look at combining in order to guarantee that they have the most effective plan possible:

Encryption

Encryption is the process of using algorithms to transform data into a form that conceals its original meaning. When data is encrypted, it guarantees that communications may only be read by the intended receivers who possess the correct decryption key. This is extremely important, particularly in the event that there is a data breach, because even if an adversary is successful in gaining access to the data, they will not be able to comprehend it if they do not have the decryption key. Tokenization is one of the options that may be utilised throughout the data encryption process. This safeguards the data while it travels through an organization's whole information technology infrastructure (Brooks, 2021).

Data Erasure

There will be times when businesses no longer require data and demand it to be erased from their servers in a manner that is irreversible. Erasing data is an efficient method for managing data security that eliminates the risk of being liable for a data breach and reduces the likelihood of a breach occurring.

Data Masking

Through the process of data masking, a company is able to conceal data by obfuscating and then substituting particular characters or numbers. If the data were to be intercepted by a hacker, this procedure, which is a sort of encryption, would render the data unusable. Only the person with the key to decrypt the message or substitute the unmasked characters will be able to read the original message.

Data Resiliency

Creating backups or copies of an organization's data is one way for that organisation to reduce the likelihood of inadvertently destroying or losing data. Backups of data are absolutely necessary in order to keep information safe and guarantee that it will never be lost. This is of utmost significance in the event of a data breach or ransomware attack, as it ensures that the firm can successfully restore a prior backup (Fortneit, 2022).

The Concept of Data Integrity

The quality and consistency (validity) of data throughout its lifecycle is what is meant by the term "data integrity." After all, compromised data is of very little use to businesses, and that's before we even get into the potential risks posed by the loss of sensitive data (Brooks, 2022). Because of this, ensuring the

data's integrity is one of the primary focuses of the majority of enterprise security solutions.

There are various ways that one's data integrity might be affected. When data is copied or transferred, it must preserve its original form and should not be modified in the interim between updates. Methods for checking for mistakes and methods for verifying data are typically counted on in order to safeguard the validity of information that is copied or disseminated without the goal of changing it. According to the hypothesis of Brooks (2021), the integrity of the data could be affected by the following:

- *Human mistake, whether willful or inadvertent*
- *Transfer mistakes, including accidental adjustments of data breach, during the migration from one device to another*
- *Bugs, viruses/malware, security breaches, and other cyber dangers*
- *Compromised hardware, such as a device or disk crash*
- *Physical compromise to devices*

In view of the fact that data security may only be able to entirely prevent a portion of these invasions, the necessity of data backup and duplication cannot be stressed in terms of safeguarding the integrity of data. Other suggested procedures to preserve data integrity encompass input validation, which helps to guarantee that incorrect information is not entered; error detection and data validation, which helps detect errors that occur during data propagation; and safety precautions, which include data loss prevention, access control, data encryption, and much more (Brooks, 2021).

Data Security and Protection in Ghana

Without the data subject's permission, processing of personal information is illegal under the Data Protection Act, 2012 (Act 843) unless such processing is (Section 20(2) of the Act) essential for the fulfilment of a deal to which the data subject is a participant, approved or mandated by law, essential to safeguard the data subject's legitimate interests, essential for the smooth performance of a statutory duty, or essential to seek the legitimate interests of the data controller or a third party.

According to Section 20(2) of the Act, a data subject has the ability to object to the handling personal data, unless such regulation explicitly limits or restricts this right. According to Section 20(3) of the Act, the person who is processing the personal data is required to stop doing so in the event that the data subject objects to the processing of the personal data. According to the Act's Section 21(1), personal data should be received directly from the individual who is the subject of the data. Nonetheless, data may be collected indirectly in some conditions, as described in Section 21(2) of the Act. These instances include: the data being stored in a public record; the data subject having wilfully made the data public; and the data subject having consented to the collection of the information from another source. Unless one of the exemptions specified in the Data Protection Act is true, such as where the individual who offered the data acknowledged to the storage of the record, or when the personal data has been preserved for historical, statistical, or research reasons, a data subject who records personal data shall not safeguard the personal data for a period beyond than is necessary for achieving the goal for which the data have been obtained and processed (Section 24 of the Act).

When the data subject grants their approval to the further processing of data, this is one of the factors that determines whether or not the further processing of the data is in keeping with the initial objective of collecting the data (Section 25 of the Act). Under the Act, it is acceptable to process personal data for the goal of safeguarding members of the public in statutory provisions stipulated circumstances, such as protecting them against loss or conduct in the delivery of banking, insurance, investing, or other financial services, or in the management of a body corporate. For example: In a similar manner, the processing is permissible when the intent is to safeguard the general public from deception or ineptitude in the delivery of expert assistance, or from misbehaviour or mismanagement in the leadership of an organisation that does not seek to profit from its activities.

The Act states that a data controller cannot disclose, use, access, procure, or reveal personal data on a data subject for purposes of direct marketing without first getting the data subject's explicit written consent. Also, a data subject has the right to request that a data controller not use any of the personal data that the data subject has submitted for direct marketing at any time by sending a notification in writing to the data controller.

Responsibility, rule of law, purpose clarity, further processing suitability, information quality, transparency, security protections, and individual consent are only some of the data privacy standards that every data controller must adhere to (OneTrust, 2022).

Factors That Can Undermine the Security and Protection of Data

The preservation and safety of data can be compromised by a wide variety of external circumstances. The following elements, according to GB Advisors (2019), are considered to be variables that weaken security.

Absence of a Secure Data Backup: The availability of data is quickly becoming one of the most valuable resources for businesses. On the other hand, it appears that many businesses do not place the priority that should be placed on the development of an information backup system. This is a very dangerous oversight since it makes it almost impossible to put any kind of resilience plan into action in the case of an attack that involves the loss of data.

Misinformed Users: Hackers with a higher level of expertise can enter a system through much smaller entry points. Sadly, in the vast majority of instances, this door is unlocked by the users themselves. 84% of all breaches in computer security are caused by human error. The danger is present regardless of whether it was done accidentally or on purpose. 2019 according to GB Advisors.

Low Investment: The security of all of the company's assets in real time necessitates the implementation of cutting-edge solutions that are regularly updated. Free security tools are risky for businesses to use since they reduce the likelihood of being able to spot unanticipated breaches from potential threats in advance. This puts the company's systems in jeopardy. Tools that require payment provide access to the most recent technological advancements and add functionality that extends beyond conventional solutions such as behaviour monitoring.

Ways of Improving Security and Protection of Data during SIM

Registration Exercise

Data are extremely valuable resources for any firm to possess. During the process of registering a SIM card, there are a number of opportunities to enhance the level of data security and protection; some of these are detailed below. Brooks (2021) discusses a few different approaches to strengthening data security.

Protect the Data Itself, Not Just the Perimeter: As much as 90 percent of a company's security budget is typically allocated to firewall technology, it would appear that the primary concern of many businesses is the protection of the data contained within their walls. On the other hand, there are potentially dozens of ways to get over a firewall, some of which include using customers, providers, or even personnel. Everyone on this list has the ability to circumvent external cyber security and abuse sensitive data. As a result of this, those who collect data need to guarantee that their efforts to secure it are concentrated on the data itself, rather than merely on the perimeter.

Pay Attention to Insider Threats: It is simple to imagine dangers coming from outside an organization because they are so frequently portrayed in the media, particularly on television and in the news, as being the gravest and most expensive dangers. The fact of the matter is, however, that those who are already on the inside have the most ability to cause you harm. Internal threats can be challenging to spot and hard to avoid because of the nature of the attacks themselves. It is imperative that data collectors be monitored to prevent any tampering with the personal information of customers.

Encrypt All Devices: In today's society, a growing number of individuals favor working on their own personal computers or mobile devices. What steps can you take to ensure that the reliability of these devices? Data collectors have the responsibility of ensuring that all data is saved in an encrypted manner and that this format is maintained throughout any migrations.

Establish Strong Passwords: There are still many firms that have lax password requirements, which results in important accounts having passwords that are simple to break as they are basic, generic, and commonly used. These accounts have access to data that is secret and critical. Strengthening the complexity of passwords is the first thing that should be done to increase the degree of security in this area. Data collectors should use passwords that are reasonably difficult and update them at least once every three months. They need to avoid using passwords like "12345" or "Admin1" at all costs. It is not an excellent plan to write down passwords and then leave them on the desktop where other people may see them.

Back-Up Data Regularly: The data collectors' overall information technology security strategy ought to already include this as an essential component. If they have reliable backups, they are able to withstand anything from the unintentional deletion of files to the entire shutdown of the system by ransomware. It is recommended that businesses keep backup copies of their data at a separate, off-site location that is both secure and distant from their principal place of business (Lepide, 2022).

Empirical Review

In order to put to rest a particular research subject, the process of conducting an empirical literature review entails the examination of prior empirical studies (Branded Content, 2022).

Research on SIM card registration in developing countries focused on the two topics, Data privacy and security (Ahmed *et al.*, 2017). In Bangladesh, where the government has just recently mandated that every mobile phone user complete mandatory biometric registration, the study was carried out through a combination of an in-person ethnography that lasted for three months and an online survey with a sample size of 606. Their investigation brought to light significant privacy and safety problems in relation to issues of identity, ownership, and trust, and shed light on the cultural and political obstacles that must be overcome in order to implement a biometric registration system in Bangladesh. They also examined the various ways in which alternate designs of infrastructure, technology, and policy could be able to better accommodate the competing interests of stakeholders in the Global South.

Mbapila (2020) examined the law and practices on the Data Protection and SIM card registration in Tanzania as provided for in the Electronic and Postal Communication Act together with the Electronic and Postal Communication Act (Regulations) and the Electronic and Postal Communication Act (consumer protection) which came with the need of having a well and trust worth method of ensuring that the SIM card users register their SIM cards and also the Registrars register the Sim card users in accordance to the requirement of the law the main concern being the issue of data protection of the individuals on SIM card. The research employed a qualitative method of

data collection which entails the primary and secondary methods of data collection. The research also went further on defining the key terms used in the research providing some insight into their actual meaning and how they have been used in the research in general.

Rumaisa (2018) investigates the personal data protection law that is utilised in the registration process for mobile phone sim cards in Indonesia. The article provided an explanation of personal data cases that were associated with mobile phone SIM card registration. Some concerns regarding the misuse of personal data were chosen as an illustration to propose regulating personal data protection. Furthermore, the article investigated why personal data is gathered, how sensitive data is collected, how much data may be collected, how long data can be stored, how it can be transferred, and how it can be deleted.

Oyediran, Omoshule, Misra, Maskeliunas, and Damasevicus (2019) conducted a study in Lagos Metropolis, Nigeria, to evaluate the perspective of mobile telecommunication users regarding the registration of SIM cards. The study adopted components from the theories of planned behaviour and reasoned action in order to better understand the perspectives of telecommunications users. In order to pick five different local government areas inside the city of Lagos, the approach of purposive sampling was used. The decision of these 300 mobile phone customers was carried out via the use of a random sampling process. It was decided that 290 out of the total amount of replies could be utilized. The analysis of the data was carried out making use of statistical processes, and Spearman's correlation analysis was applied in order to assess the relationship between the variables of interest. According to the poll's conclusions, people who use SIM cards have a good attitude toward

registering of the poll, people who use SIM cards have a good attitude toward the registration of their SIM cards. Both perceived utility and perceived simplicity of use had substantial negative correlations with subscribers' views on SIM card registration ($r = -.116$ and $r = -.132$, respectively, $p < 0.05$), suggesting that perceived usefulness and perceived ease of use significantly influenced subscribers' attitudes toward SIM card registration.

Chapter Summary

The chapter began with an introduction of the protection motivation theory which underpins this study and consequently discussed it within the context of the study. The second part of the literature review focussed on relevant themes and concepts permeating the study. Key among these concepts was, the ways of Improving Security and Protection of Data during SIM Registration Exercise. Here, Brooks (2021) discussed a few different approaches to strengthening data security such as, protecting the data itself and not just the perimeter, paying attention to insider threats, encrypting all devices, establishing strong passwords, and backing-up data regularly. The last part made an empirical review of some previous research under the study.

CHAPTER THREE

RESEARCH METHODS

Introduction

The chapter outlines the research approach, method, design, instrumentation, population and sample, data collection and data analysis technic used. This qualitative research encompassed a semi-structured interview survey designed to narrate from both subscribers' and officials' points of view of the SIM registration process and their thoughts on how secure are the data collected.

Research Philosophy/ Paradigm

Without an understanding of research philosophy, research techniques cannot be fully developed. Research philosophy can be broken down into three subfields: ontology, epistemology, and axiology. With the use of these philosophical viewpoints, they are able to decide which strategy a researcher ought to choose and why, based on the issues being asked in the research (Saunders, Lewis, & Thornhill, 2009). The research philosophy, which is comprised of the fundamental presumptions, provides an explanation of the worldview held by the researcher. Because of these presumptions, the study strategy and methodology that are used will be different.

Given the nature of this research, the ontology research philosophy is employed. Ontology is a research philosophy that is based on the nature of reality. There are two paradigms under ontology that is objectivism and subjectivism. This line of inquiry is founded on the subjectivist philosophy since its focus is on social phenomena that have arisen as a result of the perceptions

and effects of social actors who are interested with the existence of such phenomena.

Research Approach

For the purpose of gaining an understanding of a phenomenon, research is the act of collecting, analysing, and interpreting data (Leedy & Ormrod, 2001). The process of conducting research is methodical because it requires defining the purpose, organising the data, and communicating the findings to take place inside pre-existing frameworks and adhere to pre-existing rules. Researchers are given a suggestion by the frameworks and guidelines as to what components of the study should be included, how the research should be carried out, and what sorts of conclusions are likely to be formed from the data that was acquired. Research is described as the act of gathering, evaluating, and interpreting data in an attempt to acquire knowledge of a phenomena (Leedy & Ormrod, 2001). The process of doing research is systematic in the sense that it adheres to predetermined frameworks and standards in order to identify the aim of the investigation, manage the data, and communicate the findings. The frameworks and suggestions can be used by researchers to help them determine what aspects of their research to include, how to carry it out, and what kinds of conclusions are likely to be drawn from the data that was gathered.

In order to get started with research, you need to have at least one question about a subject that interests you. Researchers can better focus their ideas, better manage their efforts, and select the most effective technique or perspective to make sense of each occurrence of interest by formulating their inquiries in the form of research questions. Research that combines quantitative and qualitative methodologies, as well as hybrid methods, is becoming

increasingly common. The researcher prepares ahead and predicts the numerous sorts of data that will be required to deliver an answer to the research question. Is it required, for example, to have numerical information, textual data, or both numerical and textual data? The researcher will pick one of the three techniques to performing research depending on the outcomes of this investigation.

Researchers typically employ the quantitative method when seeking answers to research problems that can be answered with numbers, the qualitative approach when seeking answers to research questions that can be answered with text, and the mixed methodologies strategy when seeking answers to research issues that can be answered with both numbers and text. The frameworks and suggestions can be used by researchers to help them determine what aspects of their research to include, how to carry it out, and what kinds of conclusions are likely to be drawn from the data that was gathered.

This research employed a qualitative research methodology because qualitative approaches have proven to be exceptionally useful in discovering the meaning that individuals give to the circumstances that they experience (Merriam, 1998). Learning can be approached in a more comprehensive manner via qualitative research, which involves investigation. One further way to define qualitative research is as an expanding model that occurs place in a natural environment and gives the researcher the opportunity to construct a level of detail via actively participating in the real events being researched (Creswell, 1994).

There are many justifications for the adoption of the qualitative approach. First of all, the qualitative research method was adopted as it better reflects the objectives of this study to identify the processes that are involved in

the data collection and synchronization exercise and to identify the persons and institutions that are involved (directly and indirectly) in the data collection and synchronization exercise at all levels, to identify the factors that could compromise the security and protection of data and to recommend ways of improving the security and protection of data during the SIM card re-registration exercise across the country. The Qualitative approach aligns with these objectives because they are exploratory in nature. In an attempt to achieve the objectives of this study, "what", "how" and "why" questions are asked, which are all qualitative in nature.

There are a few benefits to using a qualitative research approach. The qualitative technique, for starters, generates detailed descriptions of participants' thoughts, opinions, and experiences, as well as evaluates the meanings of their activities (Denzin, 1989). Secondly, the qualitative allows researchers to learn about the inward experiences of participants as well as how they make meaning and shape them within their cultural context. (Corbin & Strauss, 2008). Finally, qualitative research methods like observation and unstructured interviews used for collecting data allow researchers to interact with participants hence there is greater flexibility.

Aside from the benefits described previously, there are some drawbacks. One of them is the problem of generalizability of research findings to the overall population, which is exacerbated by the use of small sample sizes. Due to the fact that qualitative research works best with relatively small samples, the results of such studies run the risk of being misconstrued as representing the opinions of a much broader community (Bell, 2005). In addition, completing a case study takes a great amount of time, and one can only

generalise the results to a large population in a confined way. (Flick, 2011). In conclusion, it's probable that data interpretation and analysis may be more complicated (Richards & Richards, 1994).

Study Area

This investigation was carried out in the Cape Coast Metropolitan Assembly (CCMA), which is located in Ghana. The Central Region of Ghana is governed from the city of Cape Coast, which serves as its capital. Out of the twenty-three districts that make up the Central Region, only Cape Coast can be considered a metropolitan area. The Greenwich Meridian can be found between latitudes 5 degrees 20 minutes and 1 degree 11 minutes and 41 seconds west of Cape Coast Metropolis. The Gulf of Guinea can be found to the south of the Metropolis, while the Komenda-Edina-Eguafo-Abrem District is bounded to the west, the Abura-Asebu-Kwamankese District can be found to the east, and the Twifu-Heman Lower-Denkyira District can be found to the north of the Metropolis. It has an area of roughly 122 square kilometres, with its most remote point being Brabedze, which is about 17 kilometres away from Cape Coast, the seat of both the Metropolis and the Central Region. After twenty decades of existence, the Metropolitan Assembly (CCMA) was upgraded to Metropolitan status by L.I. 1927 in February 2007. Prior to that, the Metropolitan Assembly had been created initially as a municipal Assembly by L.I. 1373 in 1987. The chance to grow the service industry is afforded to Ghana by Cape Coast's strategic location, which places it between three of the country's most important cities: Kumasi, Accra, and Takoradi. Additionally, Cape Coast serves as the educational centre and tourist center of Ghana, making it an ideal location for this purpose.

A notable attraction to Cape Coast is the number of educational institutions the metropolitan boasts of. One out of three of Ghana's premiere universities, the University of Cape Coast is found here. Also, the Cape Coast Technical University (CCTU) is located here. There are also notable second cycle institutions which include Wesley Girls High School, St. Augustine College, Mfantshipim School, Adisadel College and many more. In the centre of the city is also one of the biggest commodity markets in the country; the Kotokuraba Market. As at the 2021 population census in Ghana, the total population of the CCMA was 118,106 out of which 57,365 are males and 69,741 are females. This accounts for one of the main reasons why the CCMA was chosen as a study area. The large population and the small number of network provider offices available for SIM registration makes this study area a valid place to undertake the research.

Population

Cohen (2013) defines a research population as all the people inhabiting a specific area. People who are the focus of the research are known as the "population of interest," and they are who the study aims to analyse and perhaps help. The SIM registration centres located within the Cape Coast Metropolis constitute the population that will be contacted. According to the MoCD, the SIM registration centres include the network branches of MTN, Vodafone, AirtelTigo and Glo. It also includes all the networks connect stores, distributor branches, light retail stores and agent touchpoints of all the telecommunication networks across the country. Given these various avenues for SIM registration, the researcher was not able to ascertain the total population of the various centres within CCMA.

Sample and Sampling Procedure

In qualitative research, in principle, sample sizes shouldn't be so small that it's hard to achieve saturation in the population being studied. On the other hand, there should not be such a large number of people in the sample that it makes doing an in-depth, case-based study difficult (Sandelowski, 1995). For this study, a total of three SIM registration centres were chosen; one each representing the three major telecommunication networks in Ghana (MTN, Vodafone and AirtelTigo).

A multi-staged sampling procedure was adopted for this study. First of all, the convenience sampling method was employed to locate SIM registration centres that were close to the researcher as a result of the constraint of time and finance. Next, the purposive sampling technique was then employed for the next stage of the sampling process to determine the officials and subscribers who are to be interviewed for the study. The deliberate selection of a participant on the basis of that person's qualities is the definition of intentional sampling, which is sometimes referred to as judgement sampling. It is a method that does not choose participants randomly and does not demand any underlying ideas or a set number of participants in advance.

This requires locating and choosing individuals or a group of people who are knowledgeable and experienced in a particular area of interest in order to accomplish this goal. In addition to the respondents' knowledge and experience, an emphasis is placed on their accessibility and desire to participate, along with their capability to articulately, expressively, and reflectively share their experiences and ideas. Purposive sampling, on the other hand, seeks to concentrate on individuals who possess particular characteristics and who will

be in a better position to assist with the research than those who are included in random studies, which seek to include people of diverse ages, backgrounds, and cultures.

For this study, the researcher interviews 1 official each from the three SIM registration centres and also interviews a total of 6 subscribers; 2 from each centre. Making the total sample size of 9.

Sample Size Selection

The number of each group of the two different respondents is presented in Table 1 below. The total respondents was 9, with 6 subscribers representing about 97% and 3 officials representing (3%).

Table 1: Total number of respondents

Category	SIM registration centres	Total Number
Subscribers	MTN	2
	Vodafone	2
	AirtelTigo	2
Officials	MTN	1
	Vodafone	1
	AirtelTigo	1
Total		9

Source: Field survey, 2022

For this study, a total of three SIM registration centres were chosen; one representing each the three major telecommunication networks in Ghana (MTN, Vodafone and AirtelTigo).

Data Collection Instrument

The researcher used two main data collection instruments. The first is the use of existing literature and the other is an interview guide. The researcher also used both primary data and secondary data.

Utilizing an interview guide was the major method for collecting the data. An interview guide is vital to the success of an interview process as you can zero in on the right issues more easily and also minimizes mistakes arising from gut feelings and first impressions. Interview guides were adopted for this study because they help explore research subjects' opinions, behaviour, experiences etc. This helped us to explore the perception of the targeted sample and also discover some qualitative factors accounting for significant differences in the learning outcomes of the two delivery methods being studied. They are mostly open-ended so that in-depth information can be collected. However, interview guides can sometimes end up making the interview process rigid. That is, the researcher might focus more on the guide than the responses of the participants.

The use of secondary data from extant literature was the second data collection instrument used. These secondary sources include existing literature and online publications on the SIM re-registration exercise including its documented implementation guidelines and framework to better understand the government's rationale and modalities for this initiative and also various international and national policies on citizen's data security, protection and sharing to ascertain existing acceptable standards.

Reliability and Validity of Data and Research

The unreliability of qualitative research is an issue that is occasionally brought up in discussions about the method. The degree to which the results of an investigation may be reliably reproduced is referred to as its dependability.

Using the criteria developed by Lincoln and Guba, the researcher determined the degree to which the findings of the study might be trusted (1985). The researcher was able to lessen objections to the study's credibility by triangulating the available data. Having credibility requires establishing a connection between the findings of the research and the real world in order to demonstrate that the conclusions of the study are accurate. The legitimacy of qualitative investigations is severely hindered if they do not make use of several sources of data. As the research went on and new information became accessible, steps were made to validate each individual piece of data with at most one other source (for example, a second interview) and/or a second method (for example, an observation in addition to an interview) (Denzin, 1989; Lincoln & Guba, 1985). Results that are more accurate, comprehensive, and objective can be achieved by utilising a second source of information or technique (Silverman, 2006). Interviews and field notes were contrasted with one another so that the study's dependability could be determined.

Also, the findings of the study were exclusively based on the opinions of the officials and subscribers and also on what the extant literature posited. Thus, the findings of the study were not influenced by the researcher's personal opinions and feelings.

Data Collection Procedure

The utilization of qualitative interviews was the primary data collection method used. In certain cases, qualitative interviews are referred to as extensive or in-depth interviews. These interviews were semi-structured, in the sense that the respondents were given specific themes to discuss, but the questions were not asked in the same way or in the same order as each respondent. The researcher employed open-ended questions in which respondents were asked to react using their own words, phrases, or sentences. The interview was conducted using an interview guide that was created.

The interviews were conducted face to face. Face-to-face sessions were held at the SIM registration centres where the respondents were sited. The average length of an interview was 30 minutes. The process was tested on a few respondents before the proper data collection was initiated.

Data collected from secondary sources were also discussed thematically and presented in relation to the objectives.

Data Processing and Analysis

In understanding the data security and protection during the SIM registration exercise from the perspective of officials and subscribers, the researcher employed the use of thematic analysis.

The data were analysed using a method called thematic analysis. Thematic analysis is a strategy for evaluating qualitative data that comprises going through a data set in search of repeating themes, developing a comprehension of those themes, and then reporting on those themes (Braun and Clarke 2006). It is a way for describing the data, but it also involves interpretation of the choice of codes and the formation of themes. The versatility

of thematic analysis to be employed within a broad number of theoretical and epistemological frameworks, alongside to being applied to a large variety of research topics, research techniques, and sample sizes, is one of the distinguishing qualities of this form of study. When trying to gain a comprehensive understanding of a particular collection of events, thoughts, or behaviours throughout a data set, thematic analysis is an approach that is both appropriate and effective to utilise (Braun and Clarke 2012). Because it is intended to look for meanings that are shared or commonly held, it is not the most effective tool for investigating the singular meanings or experiences of a single individual or piece of data. Both the interview and the secondary sources of literature were analysed through the lens of the theme approach.

The thematic analysis process consists of the following phases: getting to know the data, establishing first codes, searching for themes, assessing themes, defining and identifying themes, and writing up the findings.

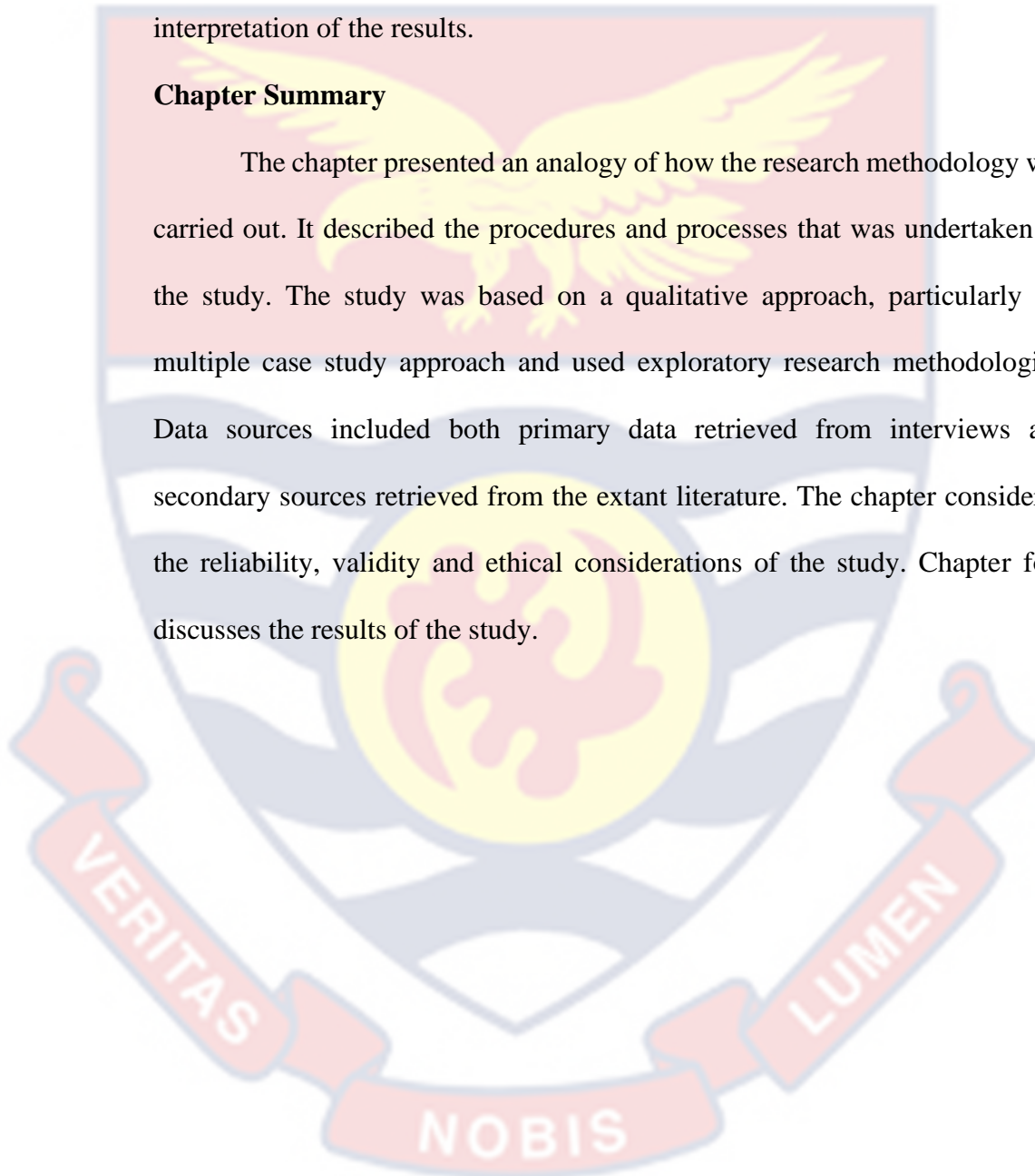
Ethical Considerations

Bryman and Bell (2007) outline some very important ethical considerations in research. Full consent of the participants was obtained before the study. Participants knowingly, voluntarily and intelligently, and clearly and manifestly, gave their consent to participate in research voluntarily. No participant was forced to participate in the study. Participants' anonymity was also protected during the study. The timing, scope, and general conditions under which participants' personal information will be shared with or withheld from us were entirely up to them. Neither they nor anyone else had their personal space invaded.

All of the guidelines established by the University's ethical standards for research have been strictly followed. A concerted effort was made to reduce the possibility of researcher bias by eliminating the possibility that the researcher's preconceived notions would influence the quality of the study or the interpretation of the results.

Chapter Summary

The chapter presented an analogy of how the research methodology was carried out. It described the procedures and processes that was undertaken by the study. The study was based on a qualitative approach, particularly the multiple case study approach and used exploratory research methodologies. Data sources included both primary data retrieved from interviews and secondary sources retrieved from the extant literature. The chapter considered the reliability, validity and ethical considerations of the study. Chapter four discusses the results of the study.



CHAPTER FOUR

RESULTS AND DISCUSSION

Introduction

This chapter entails data presentation and analysis. The main focus of the study is to analyse the data security and protection process during the national sim card registration exercise in Cape Coast, Ghana. Nine participants, of which three were officials from telecommunication network companies and six were SIM registration subscribers within the Cape Coast Metropolis were purposely sampled from the population for a face-to-face interview and 8 respondents were successfully interviewed giving a successful response rate of 88%.

In the analysis, secondary sources including existing literature and online publications on the SIM re-registration exercise are also analysed and presented in themes.

Objective One – To identify the processes that are involved in the data collection and synchronization exercise.

Under the first objective that was set for this study, the following questions were asked from network officials and subscribers involved in the SIM re-registration process, “ What is the purpose of the SIM re-registration exercise and why is it important?”, “What are the basic requirements for a person to re-register a SIM?”, “What type of information do you collect from the individuals who come for the SIM registration exercise?”, “What is the process that you take an individual through for the SIM registration?”, “After collecting the data, what electronic process does the data taken through?”, “Where is the data finally stored?”.

The main themes that emerged were the purpose of the SIM re-registration process, the basic requirements and information needed from individuals to register and the SIM registration process. They are discussed according to the interview responses and extant literature from the National Communication Authority (NCA).

Purpose of the SIM Re-registration

Subscriber 1 asserted that “Not much about it because we were not educated much on it”. Subscriber 2 also claimed “No idea”. These two respondents claimed to have no idea as to why the SIM re-registration process was being undertaken. Subscriber 3 posited that “I think it is for security reasons”, subscriber 4 also said, “They said they are connecting my Ghana Card to my SIM, apart from that I don’t know why they are undertaking this exercise.”

The 5th Subscriber said “it’s for identification purposes” and the 6th Subscriber said, “they were saying that they wanted to link it to the Ghana Card”. The first official interviewed said “what I can say is that it will help in reducing financial fraud and identity theft” and the second official said, “It helps solve fraud issues many customers encounter especially people who are using SIM cards that are not registered in their name”.

Largely, it is realized that most people believe that the main reason for the SIM re-registration is fraud, theft and security reasons. From the official website of the NCA, there are 8 major reasons for undertaking the SIM re-registration exercise.

1. Secure your SIM and stay connected

2. The second goal is to create a reliable SIM database that will inspire trust in telecommunications-reliant services and prevent malicious attacks.
3. To curb fraudulent and criminal activities
4. Secure SIM Card based transactions
5. To aid in constantly identifying the precise quantity of active, authentic SIMs on the networks
6. The activity will make it possible for operators to construct a more accurate demographic profile of their client base and will assist operators in the creation of goods and services that are tailored to the various categories of customers they serve.
7. Seventh, the data will be used by the regulator, NCA, to create statistics that would help them better control the industry.
8. The ability to use E-Government services and other private e-services means that SIM Registration will boost economic growth and progressively legalize the informal sector. Additionally, the SIM Registration would help vulnerable sectors gain access to financial services.

The third and fourth reason posited by the NCA “To curb fraudulent and criminal activities” and “Secure SIM Card based transactions” respectively corresponds to what most people think of as the reason why the exercise is being carried out. An extensive review of the NCA’s website also provides additional information as to the reasons for undertaking the SIM re-registration exercise which is tagged as “Why are re-registering?”, the following reasons were spelt out by the NCA:

1. **ID Verification** – Verifying people's identities during and after SIM registration in 2010/2011 was a major problem. Currently available SIM registration databases contain entries for both real and fabricated names and ID numbers. The lack of identity verification throughout the registration process has put at risk the existing SIM registration databases.
2. **Pre-registered SIM cards** – Furthermore, some SIM card merchants were able to register SIMs before selling them due to the lack of ID verification. As a result, the SIM card has already been activated by the time it reaches the consumer. This fundamentally undercut the aim of the SIM registration procedure. In 2016, the Electronic Communications (Amendment) Act, 2016, Act 910 barred trade in pre-registered SIMs. Offenders were and are punishable on summary conviction to a penalty of not more than three thousand penalty units or a period of jail of not more than five years or both.
3. **Non-enforcement of the provisions of the law** – Since sometime in 2013, the NCA reduced the enforcement of the SIM Registration Regulations due to an initiative to register all SIM users after the issuing of a National Identification Card. Regulation 7(1)(l) of the National Identity Register Regulations, 2012 – L.I. 2111 (20th Feb 2012) makes the National ID card the obligatory identifying document for registration of SIM cards. The aim at the time was to undertake a nationwide SIM re-registration exercise after the national ID registration effort is finished. The national ID project which was delayed generated a protracted gap in the enforcement of the SIM registration laws leading

in multiple wrongly registered SIMs being activated on the networks of the MNOs.

4. **Enforcement of the provisions of the law** – The following forms of identification are required by law to be used throughout the registration process:

- i. The National Identity Register requires individuals to use their National Identity Cards (Ghana Cards) for identification purposes during the SIM card registration process, as stated in Regulation 7(1)(l). This includes both citizens and non-citizens who are eligible for National ID Cards.
- ii. A valid passport or an ECOWAS Card is required of non-citizens who are not permanent residents of Ghana and who will be staying in Ghana for fewer than ninety days throughout the application process.
- iii. III. A certificate of incorporation will be necessary for the identification of a body that is established as a corporation.

From the review of the extant literature and interviews, it speaks that they are many reasons and rationale behind the re-registration of the SIM chief among them include for fraud and crime prevention, security of SIM card transactions and abiding by statutory requirements.

Basic Requirements and Information Needed for SIM Registration

This is the second theme under the first objective. From the interview, subscriber 1 said “Ghana Card”. The 2nd and 3rd subscriber also said the same as Subscriber 2. Subscriber 4 said “my Ghana card, my fingerprints and digital address, location”. The 6th subscriber said “to bring your Ghana card and your

SIM card, if the SIM card was not registered in your name, you would have to take it to your network provider for it to be changed before you can register your SIM” and the 5th Subscriber said, “your ID card and fingerprints, I think that was all, I don’t remember the rest”.

In the interview with the first official, the response was “You have to link your Ghana card to your telephone number. Then, you go to the nearby agent or your network provider office to reregister your SIM card. You must go along with your Ghana card and your digital address”. The second official also said, “your Ghana Card, your SIM number, you should be above 18”.

From the interview, it can be asserted that the basic requirements and information need to re-register your SIM is the ID card (Ghana Card), a valid SIM and a digital address. A review of literature from the NCA presents some requirements. It has been realized that they are different requirements depending on the type of user the person is. There are three types of users according to the NCA and each classification has different requirements.

1. Existing and Potential Individual Subscribers (Citizens) - this refers to any Ghanaian at the age of 15 and above currently using SIM card(s) or intends to use SIM card(s). The requirement of such an individual is the Ghana Card.
2. Existing and Potential Business Subscribers – this refers to any Business(es) operating in Ghana using SIM card(s) or new businesses intending to own or use SIM card(s). The requirements of such an entity are the business registration documents and the Ghana card(s) of the Director(s) or Shareholder(s).

3. Existing and Potential Foreign Subscribers – this refers to foreign residents in Ghana and foreigners on a short visit (more than 3 months). The requirements of such people are a non-citizen Ghana Card and Passport.

Reference to the information required from individuals to successfully go through the SIM registration process includes the following.

1. Last name
2. First name
3. Ghana card
4. ID number
5. Date of Birth
6. Digital address
7. Nationality
8. Sex
9. Account number (only valid for Broadband Wireless Access (BWA) subscribers)

The SIM Registration Process

From the interview, the first official said “They first have to link their telephone number to their Ghana card if they haven’t done that. Then we take a picture of the individual, scan their Ghana card front and back, scan their NFC (near field communication) and lastly scan their left and right fingers.”, the second official also said, “first of all I take their phone number and enter the renew code, then I take a picture of the person and then scan the Ghana card (front and back), I then take his/her fingerprints and the digital address.”

The 1st subscriber also asserted that “I was asked to bring my Ghana card and after that, they merge the Ghana card ID number with my telephone number. After that, a special number was given and both my right and left fingers were snapped and also a passport picture was taken and was asked to come another time. There was a little problem with the network the day so I was a little bit delayed and they later finished the process.”

The 2nd Subscriber also said, “They scan my fingers and registered my SIM card for me”. The 3rd subscriber posited that “I was part of those who registered it early so I followed the steps that were required, I dialled the number on my phone before going to the office for them to next confirmation to be done”. The 4th subscriber also said that “first of all I had to do an online registration at home; they gave us a Pin code and I undertook the process after that I went to the MTN office, formed a queue and when it got to my turn and then I went to the lady. She asked for my fingerprint for all ten fingers and then she asked for my digital address location which I gave her and my phone number.”

The 5th Subscriber said that “first of all I dialled a code on my phone and after dialling the code, I entered my name and ID number and had a confirmation on my phone that my number has been registered and that I need to go to the office to continue the procedure. So, I went to the office, made the registration of my fingerprints and gave out my ID card for verification as well. My picture was also taken. I also received confirmation as well that my SIM has been registered.” The 6th Subscriber also said “they sent public messages on TV and radio that we should start the process on our phones first by dialling *404# and then you go through the process which I don’t remember. And then

you go to the telecommunication network office where they would take your bio-metric data and photograph.”

From the review of what the respondents had to say concerning the process they were taken through, there seems to be a form of coherence across all the mobile networks in terms of the registration process even though some particular subscribers do not remember the exact process they were taken through.

A review of literature from the NCA lays down a chronological procedure for which one can successfully re-register their SIM card. It is broadly divided into two stages.

Stage One

The first stage is done on the individual's device (smartphone or cell phone) and no internet connection is needed. The process is narrated below

1. Dial *404#
2. Enter Ghana Card PIN (enter the letters and figures without the hyphens)
3. Confirm Ghana Card PIN
4. Enter Surname
5. Enter First name(s)
6. Enter your Date of Birth (DDMMYYYY-format)
7. Select Sex
8. Confirm details
9. Submit details provided after confirmation

To explain further, this is what goes on behind the scenes as explained by the NCA:

Mobile Network Operators (MNOs) verify customer ownership by comparing customer details (surname, first name(s), date of birth (DOB), and gender) with information already stored in the registration database. If there is a discrepancy between the two sets of information, the authentication process is initiated. In the event that ownership is proven, the subscriber's Ghana Card PIN and date of birth will be sent to the National Identification Authority (NIA) for verification. If validation is successful (matches), then the NIA verifies the information, transmits the Know Your Customer (KYC) dataset, and utilises the information to finish the registration process. A notification is given to the customer, and they will receive an email containing a one-of-a-kind reference number to use throughout the next phase of the registration process. In the event that validation is unsuccessful (mismatches), NIA will provide the Operator a failed report, which will only indicate the failed field (s) and the reason validation was unsuccessful. It is possible that the request will be denied if verification and ownership of the SIM cannot be verified. The customer will be forced to go to the Customer Care Centre (CCC) of their Service Provider after receiving a notification of the failure to complete the transaction.

Stage Two – Bio Capture

The Agent proceeds to capture the following via Secure Remote Access (SRA):

1. Front and Back of the Customer's Ghana Card
2. Picture of the Subscriber
3. Fingerprints of the Subscriber

After the information was successfully captured and sent to the Service Provider, the SIM card was then activated so that it could be used.

Objective Two - To identify the persons and institutions that are involved (directly and indirectly) in the data collection and synchronization exercise at all levels.

In accordance with the second objective of the study, the following questions were asked during the interview: “Which institution is responsible for this SIM registration exercise in Ghana?”, “What type of personnel are qualified to collect data from subscribers for the SIM registration?”, “To the best of your knowledge which institution(s) is/are involved in the SIM registration process?”, “Which of the above institution(s) own the data?”, “Which of the above institution(s) stores the data?”

The following themes emerged: Initiator of the SIM registration exercise, Personnel and Institutions Involved in the SIM registration exercise and Storage and Ownership of the data. They are discussed below.

Initiator of the SIM Registration Exercise

From the interview, the first official said that the initiator of the SIM registration exercise was both “the National Identification Authority (NIA) and the Ministry of Communication and Digitisation (MoD)”. The second official interviewed also said that the National Communications Authority (NCA) is the initiator of the exercise. The 1st subscriber said it was the NCA whilst the 2nd subscriber had no idea of who the initiator was. The 3rd subscriber said it is the “Ministry of Information”. The 4th subscriber also had no idea whilst the 5th and 6th subscribers said “the National Security Commission” and “the Minister of Information Cabinet”.

From the above answers, it can be realized that only two participants know the institution that initiated the SIM registration exercise which is the NCA. From the review of extant literature online, the researcher realized that the SIM registration exercise is an initiative from the government of Ghana that was executed through the NCA.

Act 524 of Parliament, which was passed in December 1996, was the legislation that led to the establishment of the National Communications Authority (NCA). This legislation has since been superseded by the National Communications Authority Act of 2008, however (Act 769). The Authority is the statutory organisation that has been given the mandate to issue licences for and regulate activities and services related to electronic communications in the country. The National Cultural Association (NCA) is governed by a board of directors consisting of nine individuals and presided over by Mr. Isaac E. Osei-Bonsu Jr. And an eleven-member top management team, with Mr. Joe Anokye serving as the organization's Director General. "Regulate the communications industry in a forward-looking and transparent manner that promotes fair and sustainable competition, stimulates innovation, encourages investment, protects the interests of stakeholders, and facilitates universal access to quality communications services for national development," is the mission statement of the NCA. Additionally, the NCA has articulated its aim as "A world-class communications regulator that promotes creative, dependable, and environmentally sustainable communication systems to satisfy the demands of stakeholders."

The services the NCA regulates include but are not limited to: 3G, Aeronautical Radio Services, Amateur Radio, Broadband Wireless Access, Communications Managed and Support Service Licence, Dealership, DTT Conformance Certification, Fixed Licence, Infrastructure Licence (Mast and Towers), Infrastructure Licence (Nationwide or Metro Fibre), Interconnect Clearing House, International Inbound Traffic, International Wholesale Carrier Licence, Internet/Public Data Service Provision, Maritime Radio Services, Microwave Authorisation, Mobile Cellular, Mobile Virtual Network Operations,

Numbering (SIM, M2M, Short codes, etc.), Public Radio Equipment (PRE) or Land Mobile Services, Radio FM Broadcasting, Submarine Cable Landing, Television Broadcasting, Type Approval, UMTS-900, Value Added Services (VAS) and VSAT Licences. These are the services the NCA regulates in Ghana.

It can be noted that from the above services they regulate, the SIM registration falls under the “Numbering (SIM, M2M, short codes, etc.) service.

The legal and regulatory framework under which the NCA operates includes three main broad frameworks which are the legislations, the regulations and the guidelines, codes and others.

Legislations

- 1. National Communications Authority Act, 2008 (Act 769)** - An Act to form the NCA as the central authority to approve and govern communications operations and amenities in the nation; and to provide for linked reasons. This Act is also designed to make provision for the objectives of connected legislation.

2. **Electronic Communications Act of Ghana, 2008 (Act 775)** - A legislation that covers concerns of electronic communications, broadcasting, the use of the electromagnetic spectrum, and similar concerns.
3. **Electronic Communications Amendment Act, 2009 (ACT 786)** - Legislation to revise the Electronic Communications Act of 2008 (Act 775) to provide a floor for the cost of incoming international data transmissions and other purposes.
4. **Electronic Transactions Act, 2008 (Act 772)** - Providing a floor for incoming international data traffic from other countries and other related topics, this bill amends the Electronic Communications Act of 2008 (Act 775).
5. **National Information Technology Agency, 2008 (Act 771)** - Creating the Information and Communications Technology Regulatory Agency of Ghana Act.
6. **Communications Service Tax (Amendment) Act, 2013 (Act 754)** - This measure addresses an increase in the Tax rate and other subjects which alters the Communications Service Tax (Amendment) Act, 2013 (Act 754).
7. **Communications Service Tax (Amendment) Act, 2019 (Act 998)** - Legislation to raise the Communications Service Tax rate and address associated concerns in the Communications Service Tax Act of 2008 (Act 754).
8. **Cybersecurity Act, 2020 (Act 1038)** - Legislation to create the Cyber Security Authority, set standards for cybersecurity operations,

encourage the growth of the field in the country, and address other connected issues.

Regulations

- 1. Electronic Communications (Rules of Procedure of the Electronic Communications Tribunal) Regulations, 2016 (L.I. 2235)** - These Regulations are enacted to provide for the norms of operation of the Electronic Communications Tribunal.
- 2. Electronic Communications (Interconnect Clearinghouse Services) Regulations, 2016 (L.I. 2234)** - These Regulations are designed to control a. Operations of network operators and service suppliers who link and channel national and international traffic via an internet clearing house b. Services of an interconnect clearing house approved by the Authority.
- 3. Electronic Communications Regulations, 2011 (L.I. 1991)** - These Regulations are issued to give weight to the requirements of the Electronic Communications Act, 2008 (Act 775).
- 4. Subscriber Identity Module Registration Regulations, 2011 (L.I. 2006)** - These Regulations are intended to provide a method for the registration of a Subscriber Identity Module for Subscribers of Network Operators.
- 5. Mobile Number Portability Regulations, 2011 (L.I. 1994)** - These Regulations are created to provide a method for customers to move from one mobile telecommunications company to another while maintaining the mobile number given by the service provider from whom the subscriber is migrating.

6. National Identification Registration Regulations 2012 (L.I. 21111) -

These Regulations are established to offer a mechanism for national identification registration.

7. Others include the Data Protection Act, 2012, the National Telecommunications Policy (NTP-2005), the National Communications Regulations, 2003 (L.I.1719), the National Broadband Policy and Implementation Strategy, the National Identification Authority Act, 2006 (Act 707) and the National Identity Register Act, 2008 (750).

Guidelines and Codes

1. **Mast & Towers Guidelines** - These regulations outline how a centralised system for approving new communication towers can be put up.
2. **Unsolicited Electronic Communications Guidelines** - For the purpose of controlling the spread of spam emails in Ghana, this was drafted. Effective August 1, 2021, the Guidelines are no longer in effect.
3. **Special Numbering Resources Guidelines** - The goal of creating this was to provide rules for the consistent and effective management of the numbering resources.
4. **Type Approval Guidelines** - In order to put into effect, the provisions of Section 3(n) of the Act, which gives the NCA the authority to certify and oversee the assessment of electronic communications equipment to determine whether or not it complies with international standards, as well as environmental, health, and safety regulations, particularly those pertaining to electromagnetic radiation and emissions, the Authorization Guidelines have been published.

5. **Guidelines for Television White Spaces (TVWS) Data Services** - These Guidelines have been implemented to prevent harmful disruptions from being received by licenced television broadcasting users while allowing data radio transmitters to function in the UHF band, which is allocated on a primary motive to broadcast television services, on frequency range and at sites where that spectrum is not designated to licenced services.

Personnel and Institutions Involved in the SIM Registration Exercise

This is the second theme in accordance with the second objective of the study. In answering the question about this theme during the interview, the first official posited “the telecommunication networks and the NIA”, and the second official also posited “the telecommunications, the NCA and the government”. The 1st subscriber also said “the various mobile network operators” whilst the 2nd subscriber had no idea. The 3rd subscriber believed that it was “the Ministry of Information and MTN”. The rest of the respondents posited that it was the telecommunication networks and or the government.

From the above, it can be deduced that the respondents have a fair idea concerning the institutions and personnel involved directly and indirectly in the SIM registration process. Whilst most of the answers they gave are true, it is not entirely exhaustive. From the review of literature across the web, an exhaustive list of institutions directly and indirectly involved in the SIM registration process is discussed below. Except for the NCA which has been discussed in previous paragraphs, the other institutions include; the Ministry of Communication and Digitization (MoCD), the National Identification Authority (NIA), the Mobile Network Operators (MNOs), the National Information Technology Agency (NITA), the Ghana Investment Fund for Electronic

Communication (GIFEC) and the Ghana Post (GP). Their function in the SIM registration exercise is discussed below.

Ministry of Communication and Digitization (MoCD) - Ministry of The Civil Service Law, 1993 (PNDCL, 327), as updated by the Civil Service (Amendment) Act, 2001 (Act 600), and Executive Instrument (EI) 6,2003, allowed for the foundation of the Ministry of Communications and Digitalization.

It is the major job of the Ministry of Communications and Digitalization (MoCD) to start and implement national policies with the objective of acquiring cost-effective information and communications infrastructure and services. This is done to increase and boost economic competitiveness per the policy parameters of the Coordinated Programme of Economic and Social Development Policies (2017-2024) - An Agenda for Jobs: Building Wealth and Equal Opportunities for Everyone. The Ministry of ICT's objective is to enable Ghana's transformation to an expertise society and a smart industry via the deliberate implementation of information and communication technology. Minister for Communication and Digitalization the Honourable Ursula Owusu-Ekuful leads up a management team of nine.

The role of the MoCD in the SIM registration exercise is that they serve as the initiating body that oversees every action being taken for the SIM registration process. In essence, the SIM registration initiative was launched by the MoCD.

National Identification Authority (NIA) - In 2003, the President's Office established the NIA with the responsibility of issuing national ID cards and overseeing the National Identification System (NIS). The National

Identification Authority Act of 2006 (Act 707) was enacted as a result to provide the organisation with the mandate it required to function. Enrolees' and applicants' privacy and personal information will be protected according to the National Identity Register Act, 2008 (Act 750), which legalises the collection of personal and biometric data.

Act 707 of the United Kingdom's Parliament created the NIA. Registration under the NIS, the creation of a national database or register, the issuance of National Identity Cards (Ghana cards), and the management of database use are all required of the government. The Authority's responsibilities include creating and maintaining a national database, issuing and promoting the use of national identification cards, and collecting, processing, storing, retrieving, and disseminating personal data on the population (Ghanaian citizens, both resident and non-resident, and legally and permanently resident foreign nationals). It is also required to provide access to information under its control to those who have a legitimate need to see it. Professor Kenneth Agyeman Attafuah serves as the NIA's Executive Secretary, and Mr. Abel Adusei, Board Chair, presides over the organization's ten-person board of directors.

Since the NIA is the institution that initiated the Ghana Card registration exercise, it is supposed to make sure during the linking of the SIM cards with the Ghana card, the information provided by the subscriber matches. They play a major role in the SIM registration exercise since they have the biometric data of the Ghana card which is needed for the successful completion of the SIM registration process.

Mobile Network Operators (MNOs) – Mobile network operators or MNOs refer to the telecommunication networks that are operating in Ghana. From the records of the NCA, the MNOs participating in the SIM registration exercise are; MTN, Vodafone, Glo and AirtelTigo. The SIM cards of individuals are issued by these companies thus, during the second stage of the SIM registration exercise, the SIM card owner is expected to visit the respective MNO to which the SIM card was issued so that the registration process can be completed. It must be noted not only the official branches of the MNOs can one register their SIM cards but also connect stores nationwide, distributor branches nationwide, light retail stores, retail centres and agent touchpoints across the country.

Ghana Investment Fund for Electronic Communication (GIFEC) - Providing under- and un-served communities with access to the internet, facilitating capacity building programmes, and promoting ICT are all responsibilities of GIFEC, a government organisation in Ghana (ICT). According to section 32 of Act 775, GIFEC's mandated operations include promoting the development of capacity-building programmes and facilitating the inclusion of information and communication technologies (ICT) in underserved and unserved communities, as well as the deployment of ICT equipment to educational, vocational, and other training institutions. The goal of the Ghana Information and Communications Infrastructure Corporation (GIFEC) is "To offer funding for the creation of general service and accessibility for all communities in Ghana, and facilitate the provision of basic telephony, internet, multimedia broadband, and broadcasting services to these neighborhoods," and the organization's vision is "To connect the digital divide

between the served and the unserved/underserved communities in Ghana." The Administrator, Mr. Prince Ofosu Sefah, heads up a ten-person management team at GIFEC.

The role of GIFEC in the SIM registration process is to provide the necessary ICT infrastructure and internet connectivity and various ICT centres across the country to facilitate the SIM registration process.

Ghana Post (GP) - As the government-owned entity in charge of postal service in Ghana, Ghana Post (also known as Ghana Post Company Limited) is a participant in the West African Postal Conference. When it first opened in 1854, Ghana Post was part of the Colonial Administration's Post and Telecommunications Department. In 1974, with the passing of NRC Decree 311, it was formally converted into a corporation. In 1993, the telecommunications division was separated from the rest of the company, and in 1995, Act 505 of 1995 was passed to legally establish the Ghana Postal Services Corporation.

Eventually, in 1995, the company changed its name to Ghana Post Company Limited in accordance with the Statutory Corporations (Conversion to Companies) Act 1993, Act 461, which mandated that certain government corporations convert to limited liability companies. Mail, courier, retail, agency, and financial services are all part of the company's for-profit offerings. Director George Afedzi Hayford serves as chairman, and director Bice Osei Kuffuor is in charge of day-to-day operations. The NCA has stated that Ghana Post's involvement in the SIM registration exercise is to assist the MoCD and the NCA with its Post Office Branches in carrying out the process nationally.

Storage and Ownership of Data

This is the last theme from the second objective of the study. When the respondents of the study were asked their opinions concerning the storage and ownership of their data this was their response. The first official said he had no idea whilst the second official believed it was the telecommunications that owned and stored individuals' data. The rest of the subscribers either had no idea or believed that it is the telecommunications and government that stored and owned the data of the subscribers.

From the review of extant literature, the NCA posits that the National Information Technology Agency (NITA) is responsible for the storage of the data. The data collected from the SIM registration exercise will be stored in a Central SIM Registry hosted by NITA. It should be noted that it is the Minister of Communication and Digitization (Hon. Ursula Owusu-Ekuful) who designated NITA to host the SIM register

The National Information Technology Agency was founded in 2008 as the Ministry of Communications' ICT policy implementation arm per Act 771. When it comes to information technology in Ghana, NITA is in charge of making sure the law is followed. Its goal is to help the government of Ghana realise the vision of e-Ghana, which is to transform the country's economy into a knowledge- and value-based one supported by cutting-edge technology. To accomplish this, the Commission has been charged with identifying, advocating, and developing innovative technologies, norms, regulations, and practises among government departments and local governments, as well as guaranteeing the sustainable growth of ICT via research & development planning and technology acquisition approaches. In order for e-Government to

thrive in Ghana, the creation of a national information technology agency is crucial. As a core element of the e-Ghana initiative, e-Government will help to increase productivity, openness, and responsibility in a number of key government departments and agencies.

The Institution is led by a ten-member management team spearheaded by the Director General, Mr Richard Okyere-Fosu. From the review of their website, NITA is the only Authorised registrar of the Government of Ghana's domain name. The objective of the National Information Technology Agency (NITA) is to become "A World-Class ICT Organization with Secure Infrastructure, Systems, and Services," while the goal is "NITA aims to provide a supportive framework for the installation and utilization of ICT by all industries, via the adoption of good policies and regulatory structure."

From the review of information posted on their official website, their services include hybrid cloud services, security services, infrastructure and facility and facility and support services. Among the hybrid cloud services includes the storage-as-a-service which the MoCD and NCA are using as their Central SIM registry. Also, from a review of their website, the company has been providing the government with eGovernment Infrastructure and creating secure payment systems for the government.

Concerning the ownership of data, the issue remains largely undecided. Whilst the NCA and MoCD stipulated that the data is being stored with NITA, the ownership of the data is not clearly expressed. A review of the NIA website shows that the NIA indicates that the Ghana card is the property of the Government of Ghana. The privacy policy of the various MNOs also indicates the SIM registration details of the individual subscriber are owned by the

subscriber but may be used by the MNO based on certain conditions. This is all the available data concerning the data ownership thus, it can be deduced that the biometric information on the Ghana card that is being linked with the SIM cards is owned by the Government of Ghana which is stored and protected by NITA.

Objective Three - To identify the factors that could compromise the security and protection of data.

In accordance with the second objective of the study, the following questions were asked during the interview: “What do you understand by data security and protection?”, “Has any of your clients had any concern(s) with data protection issues with you during your data collection exercise? Yes/No and If yes, please discuss a few concerns.”, “Do you believe the safety of data you collect could be compromised in a way? In what way?”, “From your personal experience of the SIM registration process can you say that the process ensures complete data protection?”, “Could there be instances and factors that could compromise the security and protection of user data?”, “Do you have a protocol to follow if there is a breach in the SIM registration process?”

It must be noted that only the fourth and fifth questions were asked to the subscribers whilst all the other questions were asked to the officials. The following themes emerged from the interview: the Safety Concerns of Data and Factors that could compromise the security and protection of user data.

Safety Concerns of Data

The first official in response to the question of compromise of safety of data said “Yes, taking data or information without the consent of people. People can just pull your data without your consent which doesn’t make your data private anymore” and the second official said, “well I believe everything is

possible, yes it can be compromised”. The first subscriber said in response “I am concerned about that because some of the agents can even involve in scamming” whilst the second subscriber said, “I believe my data is safe”.

Unlike the position of the second subscriber, the third subscriber said: “I think it was assured because I gave my data to a certified institution and establishment that has been there for a long time”. The fourth subscriber posited that “I cannot say the safety of my data is assured because it is like the process of you buying a new SIM card and you registering it with your ID card. Because even after registering your Mobile Money account, people can scam you and breakthrough and can get your full information so I don’t think it is safe”.

The fifth subscriber also said “I don’t think it is safe. The reason is that the person who collected my data at the office may have a different intention toward people collecting data for another purpose. The issue of cybersecurity is prevalent. So, I think in a way it could be safe and in some way to it is not safe given the measurements put in place.” The sixth subscriber also said “yes, I think it is safe. As far as it is linked with my Ghana Card only and my biometrics because it is my fingerprints that will determine whether it is me or not.”

From the above, it can be realized that both officials agreed that they could be a probability of compromise thus asserting that they are not entirely sure of the safety of the data. The concern of the subscribers has also split in two as half of them believe that their data is safe with one banking on the assurance that the institution that collected his data is reputable and has been in business for a long time. Another asserted his belief based on the fact that biometric data is unique to each individual thus to steal such information, the person needs all the unique details of that individual. The other half of the

subscribers asserted their uncertainty in the safety of the process as one took the position of not knowing the utmost intention of the official collecting the data, and as such, the official could use the data for other purposes than the initial purpose intended for the data collection. The others established their disbelief in the safety of the data collection process on the basis that the advancement of technology has also created new ways through which people can steal your data such as hacking, cybercrime and scamming.

Factors That Could Compromise the Security and Protection of Data

This is the second theme realized from the interview questions concerning the third objective of the study. The first official said “I don’t think the process ensures complete data and information protection. It is like trying to put a criminal in a maximum-security prison with all protocols but it is still possible that the prisoner can break out. Well, it depends, after entering the person’s details into the web portal and the process is done, the information vanishes. If the network is not good and you enter the info, after the person has left, the personal details of the person will still appear on the screen and this can give an opportunity for an official with ulterior motives to use that data for something else.” The second official also said “The data can be comprised so it does not ensure complete data protection. Yes, there could be instances and factors that could comprise the security and protection of user data.”

The first subscriber also said “Yes, there are factors” the second subscriber had no idea concerning the issue. The third subscriber had this to say “I was optimistic that nothing will happen to my data and I think this is new the government is trying to reduce cybercrimes so it is fine”. The fourth subscriber also said, “yes, you see we have these pre-registered SIM cards that are not in

your name but another person's name so you using that SIM card, and then they take your information as well so that could be a factor.”

The fifth subscriber said “Yes, first of all, I have seen some of the personnel undertaking the process do mistakes because I have a friend whose registration was made wrong. I also think there is a possibility of hackers stealing the data because like I said, you never know the intention of the person collecting the data so I believe that could happen”. The sixth subscriber also posited that “yes, it is possible. For Example, facial recognition so let us say someone has a picture of you and can show it. Those “Tech people” have so many ways that they can get your information like hacking.”

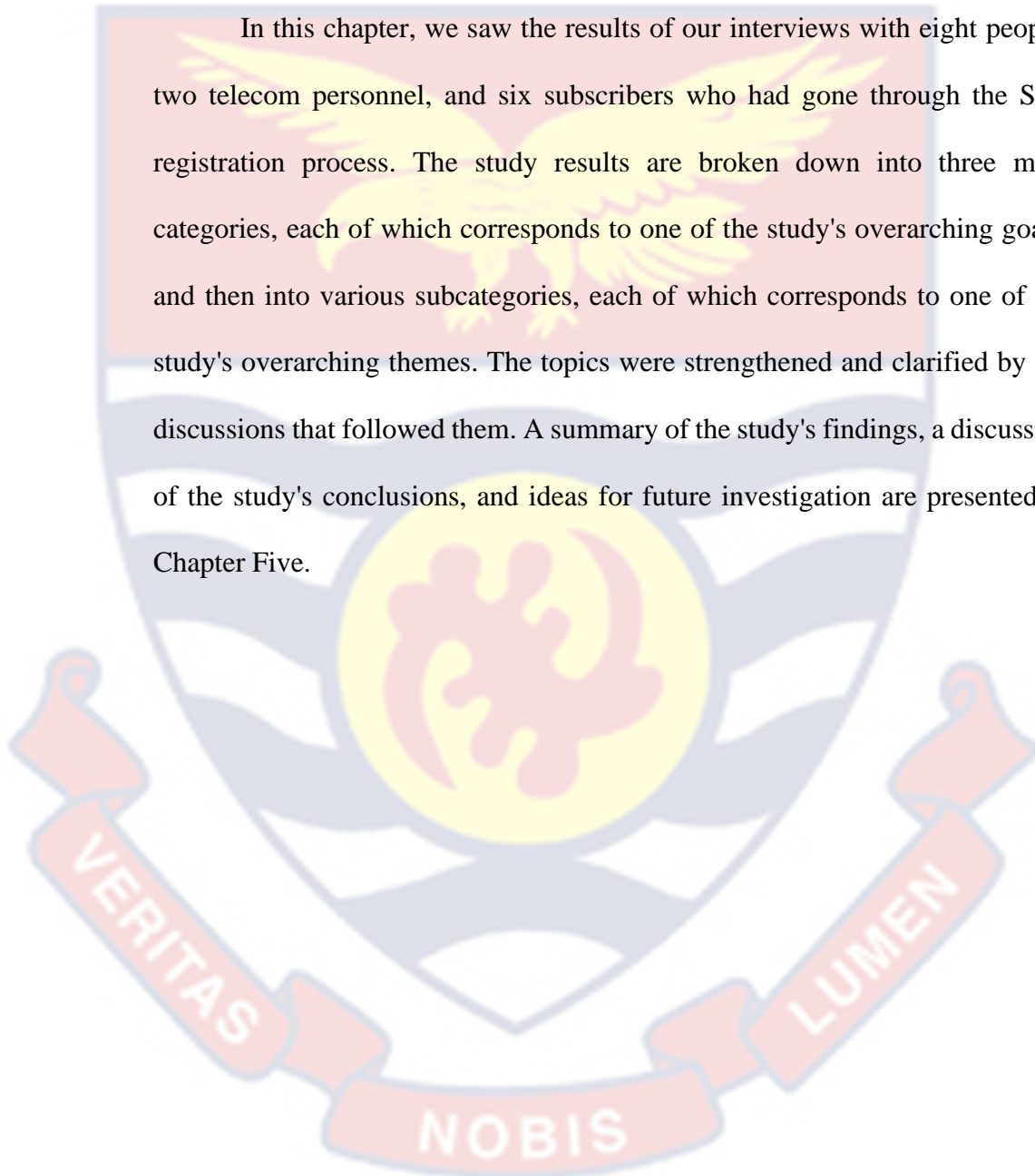
From the responses above, the first official asserts that there can be factors that compromise the data security which he asserts is based on the ineffectiveness of the platform to protect data when there is no network. When this happens, other humans can take advantage of this discrepancy to use data for their agenda. The second official though asserts that there can be factors that compromise data, he does not mention any. The first subscriber also believes that there could be instances of compromise but also fails to mention such particular instances.

Whilst the second subscriber has no idea about the issue, the third subscriber takes a different position on the issue as he has absolute confidence in the security system and believes that nothing will happen to his data. The fifth subscriber attributes the possibility of compromise to human error as he says his friend encountered such a problem during the SIM registration. The sixth subscriber also asserts that technology-enabled possibilities like hacking and cybercrime are possible. Overall, two major factors can be ascertained from the

respondents which are: human interactions whether by accident or intentional and failure or weakness in the technology system being used to record and receive the data

Chapter Summary

In this chapter, we saw the results of our interviews with eight people: two telecom personnel, and six subscribers who had gone through the SIM registration process. The study results are broken down into three main categories, each of which corresponds to one of the study's overarching goals, and then into various subcategories, each of which corresponds to one of the study's overarching themes. The topics were strengthened and clarified by the discussions that followed them. A summary of the study's findings, a discussion of the study's conclusions, and ideas for future investigation are presented in Chapter Five.



CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Introduction

The purpose of this chapter is to provide a synopsis of the empirical findings of a study conducted in Cape Coast to look at data security and protection during the national SIM card registration activity. Additionally, the chapter summarises the findings of the study and provides ideas for future study.

Summary

The study investigated data security and protection during the national SIM card registration exercise within the Cape Coast Metropolis in Ghana. To achieve this, three objectives: To identify the processes that are involved in the data collection and synchronization exercise, to identify the persons and institutions that are involved (directly and indirectly) in the data collection and synchronization exercise at all levels, to identify the factors that could compromise the security and protection of data and to recommend ways of improving the security and protection of data during the SIM card re-registration exercise across the country were set for the study from which the questions: What are the processes involved in the data collection and synchronization exercise? Which persons and institutions are involved (directly and indirectly) in the data collection and synchronization exercise at all levels? What are the factors that could compromise the security and protection of data? and What are some ways of improving the security and protection of data during the SIM card re-registration exercise across the country?

Literature relevant to the study was reviewed to help form the themes for a semi-structured interview guide to collect data. The purposive sampling method was used to select the participants who are eligible to engage in the study. In all, nine respondents were selected for the study of which eight successfully responded. The qualitative approach was employed for the study and specifically the multiple-case study approach and thematic analysis which helped to derive the understanding and opinions of others on the subject matter. The semi-structured interview guide was used to get the empirical data. Findings were derived from the transcribed data. Thematic analysis was adopted to analyse the data derived. The transcribed data and the findings were compared to other existing literature to ascertain whether the findings validate what existing literature reports. The summary of findings derived from the analysis is as follows.

In relation to the first objective of the study: To identify the processes that are involved in the data collection and synchronization exercise, there was consensus and uniformity among the participants in describing the SIM registration process even though some of them forgot the exact step by step process they were taken through. A review of the process also laid down by the NCA also shows consistency with the answers the respondents gave in the interview. Respondents also revealed that the main reasons for the SIM registration process were mainly to curb fraud, and theft and to ensure identity issues. A review of the reasons laid down by the NCA confirms the opinions of the respondents but also provides more reasons for undertaking the exercise, major among them include enforcing the provisions of the law and also securing SIM card transactions.

Considering the second objective which was to identify the persons and institutions that are involved (directly and indirectly) in the data collection and synchronization exercise at all levels. A review of the responses the interviewees gave in response to the institution responsible for the initiation, the researcher realized that most of them even though confident in their answers were wrong about it. Most ended up mentioning NIA, the MoCD and even the National Security Commission. A review of literature online asserts that the NCA is the initiator of the SIM registration process with other institutions and agencies supporting the exercise. An enquiry into other agencies directly and indirectly involved in the SIM registration process revealed that most respondents knew only their telecommunication networks and the government. A review of additional literature revealed that apart from the NCA, other institutions such as the NIA, the MoCD, MNOs, GIFEC, NITA and Ghana Post. It was also revealed that NITA stores the data collected in the exercise and is stored at the Central SIM registry with a very restricted access policy.

The third objective of the study was to identify factors that could compromise the security and protection of user data. The findings of the study revealed that whilst half of the respondents were concerned with the safety of data, the other half rest assured that their data is safe and secure with the institutions. A review of the factors they believed could compromise the security and protection of data was largely divided into two main categories: human cause and electronic or technology-based faults. In relation to the human cause, some respondents indicated it could be unintentional such as wrongful input of details whilst the other side was that those undertaking the data input could have ulterior motives for the data collection. The technology-based faults

included an inefficient system which could create the possibility of hacking, cybercrime and scamming.

Conclusions

This study was aimed at investigating data security and protection during the national SIM registration process within the Cape Coast Metropolis in Ghana. Based on the analysis and the study results, it is observed that participants gave in-depth responses to research questions and the case under study. Findings from the data revealed that the processes that respondents narrated are largely consistent with the procedures that the NCA laid down. This largely means that the MNOs are obeying what the NCA has laid down. It was also revealed that other institutions are directly and indirectly involved with the SIM registration process notable amongst them is NITA, the agency responsible for storing and securing user data and information. The study also revealed whilst some respondents had concerns about their data safety, others too were confident that their data were safe with respective institutions. Respondents also suggested that, if possible, the SIM registration process should be made in such a way that it would be possible to complete the process in the comfort and privacy of the home.

The researcher, therefore, concludes that although empirical evidence from the study indicates that respondents are largely confident in the safety of their data, more measures should be put in place to ensure maximum security and protection of user data.

Recommendations

Based on the outcome of the study and the summary of the major findings, the follow are recommendations:

1. government and respective agencies involved in the SIM registration exercise must heighten public educate on the importance of the exercise to ensure maximum cooperation,
2. officials at registration centres be trained on data security and protection best practices and be properly oriented on stakeholder roles and collaborations in ensuring maximum data security and protection at the collection stage,
3. adequate and up-to-date electronic equipment be provided at all registration centres to aid prompt and secured data collection, and
4. a secured web portal and/or mobile application be created for the public to be able to start and complete their SIM registration process from the privacy of their homes without any human intervention.

Suggestions for Further Research

The study adopted a single-case study which focused only on the Cape Coast Metropolis. Further research could adopt other designs, increase the study area and sample size for a better generalization of findings.

REFERENCES

- Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *foresight*, 20(2), 150-161.
- Ahmed, S. I., Haque, M. R., Guha, S., Rifat, M. R., & Dell, N. (2017). Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* pp. 906-918.
- Aker, J. C., & Mbiti, I. M. (2010). Mobile phones and economic development in Africa. *Journal of economic Perspectives*, 24(3), 207-32.
- Beatrice, B. (2020). *Efficacy and Challenges of Implementation of Biometric SIM card Registration by Mobile Network Operators Using the National Identification Card in Tanzania* (Doctoral dissertation, Mzumbe University).
- Bell, A. J. (2005). "Oh yes, I remember it well!" Reflections on Using the Life-Grid in Qualitative Interviews with Couples. *Qualitative Sociology Review*, 1(1), 51-67.
- Bell, D.A. (1957). *Information Theory and its Engineering Applications*. London: Pitman & Sons
- Bischoff, B. (2020). Which governments impose SIM-card registration laws to collect data on their citizens. Retrieved from <https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/>,
- Blume, P. (2010). Data Protection and Privacy—Basic Concepts in a Changing World. *Scandinavian Studies in Law. ICT Legal Issues*, 56, 151-164.

- Branded Content. (2022). “Project Chapter Two: Literature Review and Steps to Writing Empirical Review”. <https://punchng.com/project-chapter-two-literature-review-and-steps-to-writing-empirical-review/>
- Braun V, Clarke V. (2012). Thematic analysis. In: Cooper H, editor. *APA handbook of research methods in psychology*. Vol. 2, research designs. Washington (DC): American Psychological Association.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 77–101.
- Brook, C. (2020). “What is Data Integrity? Definition, Best Practices & More”. <https://digitalguardian.com/blog/what-data-integrity-data-protection-101/>
- Bryman, A. and Bell, E. (2007). *Business Research Methods*, 2nd ed., Oxford: Oxford University Press.
- Buckland, M. K. (1991). Information as thing. *Journal of the American Society for information science*, 42(5), 351-360.
- Cohen, J. (2013). *Statistical power analysis for the behavioural sciences*, 2nd edit., Routledge.
- Crabtree, B. F. & Miller, W. L. (1999). *Doing qualitative research*, 2nd edit., Thousand Oaks, CA: Sage Publications
- Creswell, J. (2009). *Qualitative inquiry and research design: Choosing among five results* (2nd edition). Thousands Oak: Sage.
- Denzin N. K., & Y. S. Lincoln (2000). *The Sage handbook of qualitative research* (3 ed., pp. 695-728). Thousand Oaks, CA: Sage Publications.
- Denzin, N. (1989). *The research acts*. Englewood Cliffs, NJ: Prentice Hall.

- Flick, U. (2011). *Introducing research methodology: A beginner's guide to doing a research project*. London: SAGE Publications Ltd.
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology, 30*(2), 407-429.
- Fortneit. (2022). "Data Security". <https://www.fortinet.com/resources/cyberGLOSSARY/data-security>
- GB Advisors. (2019). "Security Risks: What factors threaten your IT environment?". <https://www.gb-advisors.com/security-risks/>
- Great Learning Team. (2021) "4 Types of Data – Nominal, Ordinal, Discrete and Continuous". <https://www.mygreatlearning.com/blog/types-of-data/>
- GSMA (2016). Mandatory registration of pre-paid SIM cards: Addressing challenges through best practices. (April report). Retrieved from https://www.gsma.com/publicpolicy/wpcontent/uploads/2016/04/GSM-A2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf
- GSMA, (2011). "African Mobile Observatory 2011," at <http://www.gsma.com/publicpolicy/wpcontent/uploads/2012/04/africamoewebfinal.pdf>, accessed 03 August 2022.
- Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). A theory on information security.
- Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). Communication and persuasion.
- Izuogu, C. E. (2010). Data protection and other implications in the ongoing SIM card registration process. Available at SSRN 1597665.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical research: planning and design*, Merrill Prentice Hall. *New Jersey*.

Lincoln, Y., & Guba, E. G. (1985). *Naturalistic inquiry*. Newbury Park, CA: Sage.

Martin, A., & Taylor, L. (2021). Exclusion and inclusion in identification: Regulation, displacement and data justice. *Information Technology for Development*, 27(1), 50-66.

Matthew R, (2011). "Africa is world's second most connected region by mobile subscriptions," *informa telecoms & media* (3 November), at <http://blogs.informatandm.com/3485/press-release-africa-is-world%E2%80%99ssecond-most-connected-region-by-mobile-subscriptions>, accessed 03 August, 2022

Mbapila, N. J. (2020). *Examination of the Laws and Practices on Data Protection and Sim Card Registration in Tanzania* (Doctoral dissertation, Mzumbe University).

Meredith B. (2012). "How mobile puts business at the tip of Africa's fingers," *BBC News* (2 July), at <http://www.bbc.co.uk/news/business-18643549>, accessed 03 August, 2022.

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

Murphy, D. (2022). "10 ways to improve data security" <https://www.lepide.com/blog/ten-ways-to-improve-data-security/>

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. *Predicting and changing health behaviour: Research and practice with social cognition models*, 3, 70-106.

- OneTrust. (2022). “Ghana- Data Protection Overview” (<https://www.dataguidance.com/notes/ghana-data-protection-overview/>)
- Oyediran, O., Omoshule, A., Misra, S., Maskeliūnas, R., & Damaševičius, R. (2019). Attitude of mobile telecommunication subscribers towards sim card registration in Lagos State, Southwestern Nigeria. *International Journal of System Assurance Engineering and Management*, 10(4), 783-791.
- Yin, K. (2003). *Case study research: Design and methods* (3rd edition). Applied social methods series.
- Richards, T. J., & Richards, L. (1994). Using computers in qualitative research. In N. Denzin, & Y. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 445-462). London: Sage Publications.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, 91(1), 93-114.
- Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.
- Rumaisa, D. (2018). Personal Data Protection Law Used in Mobile Phone Sim Card Registration in Indonesia. *Notaire*, 1(2), 269-284.
- Sandelowski, M. (1995). Qualitative analysis: What it is and how to begin. *Research in Nursing and Health*, 18, 371–375. doi:10.1002/nur.4770180411
- Silverman, D. (2006). *Interpreting Qualitative Data*. (3rd ed.). London: Sage Publications, Inc.

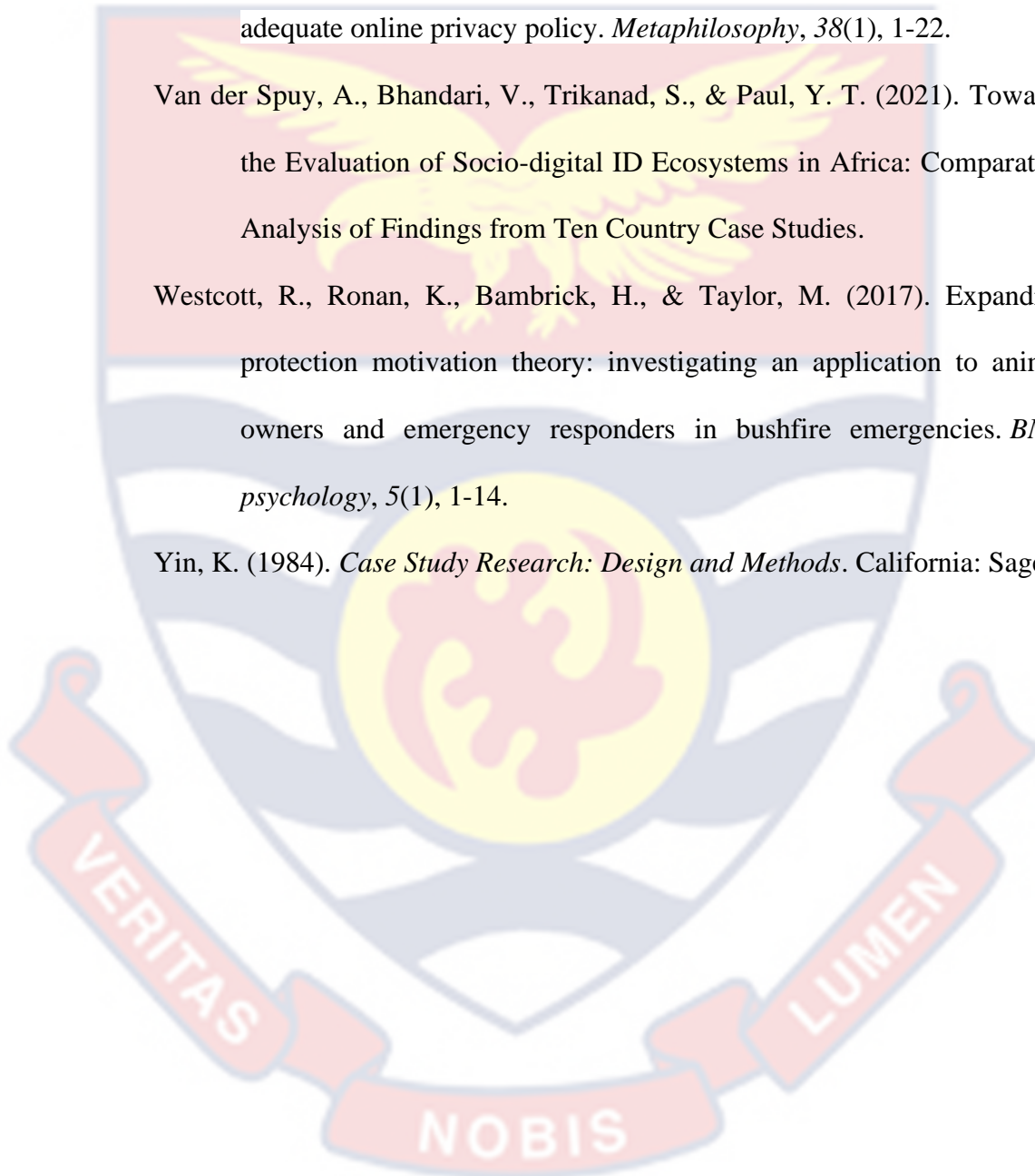
Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (2 ed.). Thousand Oaks, CA: Sage Publications.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1-22.

Van der Spuy, A., Bhandari, V., Trikanad, S., & Paul, Y. T. (2021). Towards the Evaluation of Socio-digital ID Ecosystems in Africa: Comparative Analysis of Findings from Ten Country Case Studies.

Westcott, R., Ronan, K., Bambrick, H., & Taylor, M. (2017). Expanding protection motivation theory: investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC psychology*, 5(1), 1-14.

Yin, K. (1984). *Case Study Research: Design and Methods*. California: Sage



APPENDICES

APPENDIX 1: INTERVIEW GUIDE FOR SIM REGISTRATION

OFFICIALS

UNIVERSITY OF CAPE COAST

COLLEGE OF HUMANITIES AND LEGAL STUDIES

SCHOOL OF ECONOMICS

MSE DATA MANAGEMENT AND ANALYSIS

**TOPIC: DATA SECURITY AND PROTECTION DURING THE
NATIONAL SIM CARD REGISTRATION EXERCISE, A CASE STUDY
WITHIN THE CAPE COAST METROPOLIS, GHANA**

My name is David Akoto Minta, a master's student at the university of Cape Coast reading data management and analysis. As part of my academic work, I am conducting a study to explore how the issues of data security and protection are ensured during the national SIM registration exercise. Kindly spare the researchers few minutes of your time and respond to the following questions based on your knowledge, experience and opinion on the subject matter. Information provided by any responded is strictly meant for academic purposes and will be treated with the utmost confidentiality.

FOR SIM REGISTRATION OFFICIALS

Objective One

To identify the process that are involved in the data collection and synchronization exercise.

1. What is the purpose of the SIM re-registration exercise and why is it important?
2. What are the basic requirements for a person to re-register a SIM?
3. What type of information do you collect from the individuals who come for the SIM registration exercise?
4. What is the process that you take an individual through for the SIM registration?
5. After collecting the data, what electronic process does the data taken through?
6. Where is the data finally stored?

Objective Two

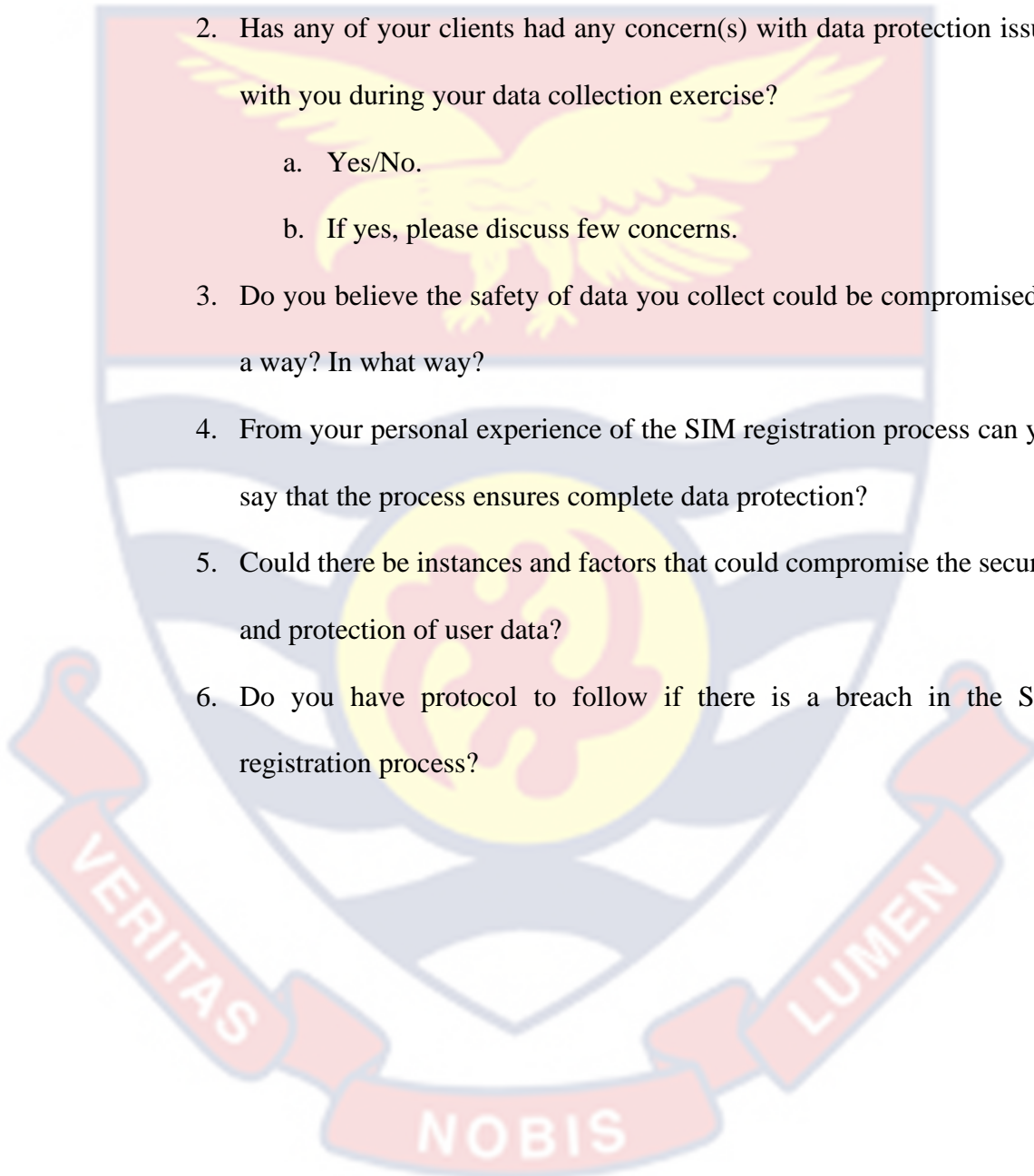
To identify the persons and institutions involved (directly and indirectly) in the data collection exercise at all levels.

1. Which institution is responsible for this SIM registration exercise in Ghana?
2. What type of personnel are qualified to collect data from subscribers for the SIM registration?
3. To the best of your knowledge which institution(s) is/are involved in the SIM registration process?
4. Which of the above institution(s) own the data?
5. Which of the above institution(s) stores the data?

Objective Three

To identify the factors that could compromise the security and protection of data.

1. What do you understand by data security and protection?
2. Has any of your clients had any concern(s) with data protection issues with you during your data collection exercise?
 - a. Yes/No.
 - b. If yes, please discuss few concerns.
3. Do you believe the safety of data you collect could be compromised in a way? In what way?
4. From your personal experience of the SIM registration process can you say that the process ensures complete data protection?
5. Could there be instances and factors that could compromise the security and protection of user data?
6. Do you have protocol to follow if there is a breach in the SIM registration process?



APPENDIXES 2: INTERVIEW GUIDE FOR SIM REGISTRATION

SUBSCRIBERS

UNIVERSITY OF CAPE COAST

COLLEGE OF HUMANITIES AND LEGAL STUDIES

SCHOOL OF ECONOMICS

MSE DATA MANAGEMENT AND ANALYSIS

**TOPIC: DATA SECURITY AND PROTECTION DURING THE
NATIONAL SIM CARD REGISTRATION EXERCISE, A CASE STUDY
WITHIN THE CAPE COAST METROPOLIS, GHANA**

My name is David Akoto Minta, a master's student at the university of Cape Coast reading data management and analysis. As part of my academic work, I am conducting a study to explore how the issues of data security and protection are ensured during the national SIM registration process. Kindly spare the researchers few minutes of your time and respond to the following questions based on your knowledge, experience and opinion on the subject matter. Information provided by any responded is strictly meant for academic purposes and will be treated with the utmost confidentiality.

FOR SIM REGISTRATION SUBCRIBERS

Objective One

To identify the process that are involved in the data collection and synchronization exercise.

1. Do you know why you are re-registering your SIM card?
2. What were the requirements for you to register your SIM card?
3. Can you narrate the processes you went through in order to successfully re-register your SIM card?

Objective Two

To identify the persons and institutions involved (directly and indirectly) in the data collection exercise at all levels.

1. Which institution in Ghana initiated the SIM re-registration exercise?
2. Do you know which type of personnel are qualified to collect data from you?
3. To the best of your knowledge do you know which institutions are involved in the SIM registration exercise?
4. Do you know the institution(s) that own your data?
5. Do you know which institution(s) that store your data?

Objective Three

To identify the factors that could compromise the security and protection of data

1. Do you think your data safety is assured given the way that the SIM registration exercise is being carried out?
2. Are there factors (human or electronic based) that could compromise the security and safety of your data?