AN EXPLORATION OF BIOMETRIC-BASED SOLUTION IN COMBATING MOBILE FRAUD AT SOUTH AFRICAN BANKING RISK INFORMATION CENTRE

by

MOKOPANE CHARLES MARAKALALA

Submitted in accordance with the requirements for the degree of

DOCTOR OF PHILOSOPHY IN CRIMINAL JUSTICE

in the subject of

FORENSIC INVESTIGATION

POLICE SCIENCE, FORENSIC SCIENCE AND TECHNOLOGY

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor

DR AVHASHONI CYNTHIA MADZIVHANḐILA

08 October 2024

DECLARATION

Student Name: **Mokopane Charles Marakalala**

Student Number: **46691022**

I declare that this thesis, **An Exploration of Biometric-Based Solution in Combating Mobile Fraud at South African Banking Risk Information Centre**, is my original work and that all sources I have used or quoted have been indicated and acknowledged by means of complete references. This is a literature study, and I further declare that no official document for SABRIC or any other institution was perused.



Mokopane Charles Marakalala
Date: 08/10/2024

DEDICATION

This study is dedicated to **St. Engenas Zion Christian Church and the Lordship of his Grace Right Reverend Bishop Dr Engenas Joseph Lekganyane, Bakwaduba**. Also, to my grandmother, the late Florah Raesibe Ngobeni and my mother, the late Ledile Margaret Marakalala, for paving an educational way for me, always encouraging me, and saying that education is the future. I will forever be grateful to my God and family, and the friends who were with me during my PhD journey. I also dedicate this thesis to Dr Avhashoni Cynthia Madzivhandila, as well as the former supervisor, the late Prof Trevor Budhram and to all colleagues in the Police Practice Department and College of Law for their positive encouragement and valuable support.

ACKNOWLEDGEMENTS

I acknowledge with gratitude the following people: without whose valuable contribution my study would never have been possible.

- Firstly, I acknowledge blessings from **St. Engenas Zion Christian Church and his Lordship Right Reverend Bishop Dr Engenas Joseph Lekganyane, Bakwaduba.**
- I would like to express my sincere appreciation towards my supervisor, Dr Avhashoni Cynthia Madzivhandila for her advice and support throughout this study. Your guidance has been invaluable.
- My former supervisor the late Prof Trevor Budhram, for his positive encouragement and expert guidance.
- My uncle, Lesiba Piet Marakalala and my aunts for valuable support.
- My dearest grandmother, the late Florah Raesibe Ngobeni and the late Ledile Margaret Marakalala for their motherly love and support, brothers and sisters. To my family, thank you for your inspiration and encouragement. You have motivated me to make a success of this.
- The University of South Africa for assisting me with study assistance during my study period.
- My line manager Prof Angela Mabudusha for excellent support and guidance.
- All colleagues in the College of Law, School of Criminal Justice-Department of Police Practice at University of South Africa.

SUMMARY

This study focuses on exploration of biometric-based solutions in combating mobile fraud at the South African Banking Risk Information Centre (SABRIC). Hackers gain access to a mobile device and use it to access accounts and confidential personal data. Online banking is used by millions of people worldwide to complete routine bank transactions quickly and easily and criminals have ample opportunities to commit this kind of fraud. The literature review from SABRIC, Association of Certified Fraud Examiners (ACFE), Global System for Mobile Communications Association (GSMA), Internet Service Providers Association (ISPA), the International Criminal Police Organisation (INTERPOL) and the Auditor-General of South Africa (AGSA) annual statistical reports from 2018/2022) clearly indicate the prevalence of successful mobile fraud and how easily cybercriminals can hijack a mobile device and use it to gain access to sensitive personal data and accounts.

A qualitative method was adopted to fulfil the purpose of the study. Non-probability sampling was used to select documents that were used to collect data, as this is a literature review study that mainly used secondary data as a source of information, including relevant national and international literature, about the biometric technology to combat mobile fraud in the South African Banking Industry (SABI). The researcher wanted to generate new knowledge with the purpose of empowering in-house investigators who investigate mobile fraud cases in the SABI. The purpose of this narrative literature review was to explore, analyse, describe the situation, and then suggest and recommend solutions to the problem identified. The information obtained from secondary data was analysed thematically. This study explores the biometric-based solution in combating mobile fraud at SABRIC. Following that, the findings indicated that the lack of online fraud expertise may lead to banks having weak detection systems. There is a lack of law regulation which poses high risks. Furthermore, this kind of study was necessary because it provides relevant information to investigators for:

- Investigative linkage of unsolved cases using biometric-based solutions in combating mobile fraud in the SABI;
- The development of investigative leads and suspect identity in unsolved cases by accumulating mobile fraud cases;
- To develop the forensics models for biometrics payments technology and digital payments techniques to combat mobile fraud.

Keywords: *Automated Teller Machine, Banking, Biometrics-Based Solution, Combat, Fraud, Hacker, Mobile Application, Mobile Fraud, Perpetrator, Sim Swap.*

LIST OF ABBREVIATIONS AND ACRONYMS

AA	Amendment Act
ABSA	Amalgamated Banks of South Africa Limited
ACFE	Association of Certified Fraud Examiners
AGSA	Audito-General South Africa
AI	Artificial Intelligence
AO	Authorisation to Operate
APP	Authorised Push Payment
ATM	Automated Teller Machine
ATO	Authorisation to Operate
BA	Banks Act
CDD	Customer Due Diligence
CFE	Certified Fraud Examiner
CJS	Criminal Justice System
CNP	Card Not Present
COGTA	Cooperative Governance and Traditional Affairs
COMRiC	Communications Risk Information Centre
CoP	Confirmation of Payee
COVID-19	Coronavirus Disease 2019
CSC	Common and Secure Communication
DigiFI	Digital Identification and Finance Initiative
EU	European Union
FATF	Financial Action Task Force
FDA	Fraud Detection Algorithms
FDT	Fraud Diamond Theory
FFAC	Financial Fraud Advisory Council
FICA	Financial Intelligence Centre Act
FICAA	Financial Intelligence Centre Amendment Act
FIU	Financial Intelligent Unit
FNB	First National Bank

FPS	Faster Payments Service
FTT	Fraud Triangle Theory
GITOC	Global Initiative Against Transnational Organised Crime
GMPC	General Multi-Purpose Cards
GPS	Global Positioning System
GS	Google Scholar
GSMCA	Global System for Mobile Communications Association
ICASA	Independent Communications Authority of South Africa
ICT	Instant Credit Transfer
ID	Identity Book
ILP	Intelligence-Led Policing
IMEI	International Mobile Equipment Identity
IMSI	Internal Mobile Subscriber Identity
INR	International Normalised Ratio
INTERPOL	International Criminal Police Organisation
IP	Internet Protocol
IPS	Instant Payment Systems
IRMSA	Institute of Risk Management South Africa
KPMG	Klynveld, Peat, Marwick, Goerdeler
KYC	Know Your Customer
MF	Mobile Fraud
MFA	Multi-Factor Authentication
MFS	Mobile Fraud Services
ML	Machine Learning
MMT	Modern Monetary Theory
MNO	Mobile Network Operators
MO	*Modus Operandi*
NACAC	National Anti-Corruption Advisory Council
NDP	National Development Plan
NGN	Next-Generation Networks
NHS	National Health Service

NIMC	National Identity Management Commission
NIN	National Identification Number
NPA	National Prosecuting Authority
OBS	Ombudsman for Banking Services
OECD	Organisation for Economic Cooperation and Development
OTP	One-Time Password
PASA	Payments Association of South Africa
PCCAA	Prevention and Combating of Corrupt Activities Act
PEPs	Politically Exposed Persons
PFMA	Public Finance Management Act
PPE	Personal Protective Equipment
PSD	Payment Services Directive
PwC	PricewaterhouseCoopers
QDA	Qualitative Data Analysis
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
RTS	Regulatory Technical Standards
RVN	Random Verification Number
SABI	South African Banking Industry
SABRIC	South Africa Banking Risk Information Centre
SAFPS	Southern African Financial Prevention Service
SALC	South African Law Commission
SAR	Suspicious Activity Reporting
SCA	Strong Customer Authentication
SDK	Software Development Kit
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
SOC	Security Operations Centre
UIF	Unemployment Insurance Fund
UK	United Kingdom
UKFA	United Kingdom Fraud Act

UNESCO	United Nations Educational, Scientific, and Cultural Organisation
UNISA	University of South Africa
UPI	Unified Payments Interface
URL	Uniform Resource Locator
WWW	World Wide Web

TABLE OF CONTENTS

DECLARATION…….....ii

DEDICATION…….....iii

ACKNOWLEDGEMENTS…….....iv

SUMMARY……..……v

KEYWORDS…….....v

LIST OF ABBREVIATIONS AND ACRONYMS……...vi

CHAPTER ONE: GENERAL ORIENTATION

1.1 INTRODUCTION……1

1.2 BACKGROUND OF THE STUDY……..2

1.3 PROBLEM STATEMENT……...3

1.4 RESEARCH AIM AND OBJECTIVES OF THE STUDY……...10

1.4.1 Research Aim……....10

1.4.2 Research Objectives……....10

1.5 RESEARCH QUESTION……...11

1.6 DEFINITION OF KEY CONCEPTS……12

1.6.1 Biometric-Based Solution……12

1.6.2 Mobile Fraud……13

1.6.3 Fraud……13

1.6.4 Mobile……...13

1.6.5 Forensic Investigation……...13

1.6.6 Combat……..14

1.6.7 SIM Swap Fraud……14

1.6.8 Digital Banking Fraud……...14

1.7 VALUE OF THE STUDY.....15

1.7.1 Value for the Academia……15

1.7.2 Value for the South African Banking Industry……..15

1.7.3 Value for the Law Enforcement……16

1.8 SUMMARY 16

CHAPTER TWO: RESEARCH METHODOLOGY AND DESIGN

2.1 INTRODUCTION.....17

2.2 RESEARCH APPROACH 17

2.3 THE PHILOSOPHICAL WORLDVIEW 19

2.3.1 The worldviews……19

2.3.2 Distinctive Methods and Subtypes……20

2.4 STUDY LOCATION.....21

2.5 TARGET POPULATION AND SAMPLING.....22

2.5.1 Study Population……...22

2.5.2 Sampling Procedures……23

2.6 DATA COLLECTION 23

2.7 DATA ANALYSIS 25

2.8 METHODS TO ENSURE TRUSTWORTHINESS.....27

2.8.1 Credibility……27

2.8.2 Transferability……...27

2.8.3 Dependability……27

2.8.4 Conformability……..28

2.9 ETHICAL CONSIDERATIONS 28

2.10 SUMMARY 29

CHAPTER THREE: THE PREVALENCE OF MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

3.1 INTRODUCTION.....30

3.2 AN OVERVIEW OF MOBILE FRAUD IN THE SABI 30

3.2.1 Forms of mobile fraud……...33

3.2.2 The techniques used in the commission of mobile fraud……..34

3.3 LEGISLATIVE FRAMEWORK OF MOBILE FRAUD.....44

3.3.1 Financial Intelligence Centre Act (No. 38 of 2001)……...44

3.3.2 Public Finance Management Act (No. 1 of 1999)……47

3.3.3 Prevention and combating of Corrupt Activities Act (No. 12 of 2014)……47

3.3.4 Banks Act (No. 94 of 1990)……..48

3.3.5 Fraud Act 2006……..49

3.4 SUMMARY 51

CHAPTER FOUR: FACTORS CONTRIBUTING TO MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

4.1 INTRODUCTION 52

4.2 FACTORS CONTRIBUTING TO MOBILE FRAUD IN THE SABI.....52

4.2.1 Corruption……52

4.2.2 Unemployment and Poverty in the South African Society……..55

4.2.3 Climate Change Relating Crime of Mobile Fraud……56

4.2.4 Substance Abuse……..60

4.3 SUMMARY.....60

CHAPTER FIVE: CHALLENGES ENCOUNTERED BY FORENSIC INVESTIGATORS IN INVESTIGATING MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

5.1 INTRODUCTION.....61

5.2 THE CHALLENGES ENCOUNTERED BY THE FORENSIC INVESTIGATORS IN THE INVESTIGATION OF MOBILE FRAUD IN THE SABI 61

5.3 THE FUTURE OF MOBILE FRAUD.....64

5.4 SUMMARY 67

CHAPTER SIX: BEST PRACTICES BY DEVELOPING A CONCEPTUAL MODEL TO COMBAT MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

6.1 INTRODUCTION.....68

6.2 THE BEST PRACTICES IN COMBATING MOBILE FRAUD.....68

6.3 THE USE OF FRAUD DETECTION TECHNIQUES 73

6.4 THE FORENSIC INVESTIGATION FRAMEWORK MODELS TO COMBAT MOBILE FRAUD 83

6.4.1 Supervised Learning Used in Fraud Detection Algorithms……...84

6.4.2 Unsupervised Learning Used in Fraud Detection Algorithm……84

6.4.3 Factors explaining why Machine Learning techniques are so popular and widely used in industries for detecting frauds……85

6.4.4 Mobile Fraud Ecosystem……...89

6.4.5 Analysis of the Existing Models……93

6.4.6 Proposed Conceptual Models for Mobile Fraud Detection……94

6.5 SUMMARY 101

CHAPTER SEVEN: PRESENTATION AND INTERPRETATION OF THE RESEARCH FINDINGS

7.1 INTRODUCTION.....102

7.2 EMERGING THEMES OF PERTINENT TO AN EXPLORATION OF BIOMETRIC-BASED SOLUTION IN COMBATING MOBILE FRAUD 102

7.2.1 Theme 1: The Prevalence of Mobile Fraud in the SABRIC……106

7.3.2 Theme 2: Factors Contributing to Mobile Fraud at SABRIC……..109

7.3.3 Theme 3: The Challenges Encountered by the Forensic Investigators in the Investigation of Mobile Fraud at SABRIC……..113

7.3.4 Theme 4: The Best Practices to Combat Mobile Fraud at SABRIC……119

7.4 SUMMARY 120

CHAPTER EIGHT: SUMMARY, RECOMMENDATIONS AND CONCLUSION

8.1 INTRODUCTION.....121

8.2 SUMMARY 121

8.3 RECOMMENDATIONS.....123

8.3.1 Common Uses of Biometric Verification**……124**

8.3.2 Mokopane Fraud Model-24: Financial Fraud Strategy**……129**

8.4 LIMITATIONS OF THE STUDY 131

8.4.1 Lack of Data**……131**

8.4.2 Narrative literature review (Annual Statistical Reports-2018/2022)**……...131**

8.4.3 Time Constraints**……132**

8.4.4 Generalisation**……132**

8.5 RECOMMENDATIONS FOR FURTHER RESEARCH.....132

8.6 CONCLUSIONS 133

LIST OF REFERENCES……134

LIST OF TABLES

Table 1.1: Mobile Fraud Allegations from 2018-2022…….....5

Table 7.1: Main/ Global Themes and Sub-Themes Generated from the Findings ……105

LIST OF FIGURES

Figure 1.1: Irregularities of a Biometrics-Based Solution to Combat Mobile Fraud…….....7

Figure 1.2: Digital Banking Fraud……...…….....9

Figure 6.1: Top 8 Best Practices to Combat Mobile Fraud……...…68

Figure 6.2: Banking App Kidnappings Profiling…….74

Figure 6.3: The Fraud Detection Algorithms Machine Learning…….85

Figure 6.4: Models for Detecting Fraudulent Mobile Fraud Transaction…….91

Figure 6.5: Conceptual Models for Detection of Mobile Fraud…….....95

Figure 6.6: The Fraud Triangle…….....97

Figure 7.2: Biometric Payment Technology in the Banking Industry ……..…110

Figure 7.3: Grayscale Photo…….....116

Figure 8.1: Mokopane Fraud Model-24…….....127

LIST OF ANNEXURES

ANNEXURE A:- DOCTORAL DEGREE (PhD) BY PUBLICATIONS…….....146

ANNEXURE B:- ETHICAL CLEARANCE…….....148

ANNEXURE C:- LANGUAGE AND TECHNICAL EDITOR CERTICATE OF COMPLETION…….....151

ANNEXURE D:- TURNITIN DIGITAL RECEIPT……..…152

ANNEXURE E:- SABRIC MAP LOCATION…….....153

CHAPTER ONE

GENERAL ORIENTATION

1.1 INTRODUCTION

The study focused on the South African Banking Industry (SABI), exploring financial crime statistics and trends by SABRIC. SABRIC is a non-profit organisation established by South African banks with the aim of helping the banking and cash-in-transit sectors combat organised bank-related crimes. Its main objective is to identify, stop, and lessen organised crime in the banking sector by means of successful public-private partnerships. It serves as a primary liaison between the banking sector and other pertinent parties such as law enforcement and regulatory agencies. The major four banks in South Africa are Nedbank, First National Bank (FNB), Amalgamated Banks of South Africa (ABSA), Standard Bank (STD) and Capitec, which together make up about 90% of the banking industry's assets.

This banking industry stands out in Africa and worldwide because of its world-class organisations and creative financial solutions. As a result, this literature study explore how biometric methods are used at SABI to prevent mobile fraud by studying existing and available literature. The issue covered in this study was the rising incidence of mobile fraud in the South African banking industry as a result of inadequate identification methods for credentialing individuals who perpetrate mobile fraud deception. The perceived usefulness, biometrics payments technology and perception of forensic models were recently identified in a study as factors that affect how users feel about biometric technology. According to the SABRIC annual report for 2028/2022, attitude was a major element influencing how well biometrics technology may be used to prevent mobile fraud. The issue of mobile fraud and the use of biometrics-based solutions to lessen control were the main focus of this research. Online banking is provided by the banking industry to make banking services more accessible and convenient for their customers. Fraudulent behaviour is becoming more common every day as the majority of banking services is now conducted online and scams are becoming more common worldwide, damaging both banks and customers.

This chapter describes the background of the study, problem statement, research aim and objectives, as well as the research questions. Furthermore, key concepts are defined, and the value of the study is highlighted.

1.2 BACKGROUND OF THE STUDY

In recent history, deep learning techniques have contributed significantly to the detection of fraud in SABRIC networks (SABRIC, 2019:np). In fact, professionals in fraud detection acknowledge that such techniques are strong, dependable, and exciting while seemingly an anomaly detection method (ACFE, 2019:np). Across the world, communication was changed by the introduction of mobile telephones followed by mobile phones which are also used to provide financial services at SABRIC. The latter approach brought financial services closer to the general public in that they could utilise local merchant infrastructure that was already in place. The use of mobile phones in banking, as reported by the Association of Certified Fraud Examiners [ACFE] (2018:np), has led to mobile fraud, which is a problem affecting the banking sector. This type of financial fraud manifests through hackers gaining access to a mobile device and using it to access accounts and confidential personal data. Online banking is used by millions of people worldwide to perform bank transactions quickly and easily.

The SABI and major companies involved in commercial crime are among SABRIC's customers. SABRIC also educates the public on self-defence techniques and increases public awareness of crimes involving bank sectors. Financial crimes prioritised by the SABRIC include fraud, money laundering, financing of terrorism, and cybercrime. Essential tasks of the SABRIC are to alert public awareness on various bank-related crimes and teaching people self-defence techniques. To fight financial crime, SABRIC encourages cooperation amongst regulatory agencies, payment processors, financial institutions, and other partners. In addition, SABRIC makes it easier to exchange information about new threats and illegal activities.

Reports published by the SABRIC showing annual crime statistics from 2018 to 2022 offer valuable information about the patterns and categories of financial crimes that took place in the banking industry in South Africa. Examples inter alia, include financial crimes of all kinds, contact crimes, card fraud and digital fraud. Also covered in SABRIC annual reports are financial losses brought about by these crimes and the measures taken to prevent them. Furthermore, SABRIC annual reports discuss the need for ongoing innovation and defence strengthening, and caution on increasingly ingenious ways in which criminal tactics are changing. A report published in 2023 by the SABRIC indicates an increase in financial crimes, leading to the loss of nearly R3 billion (SABRIC, 2023:np). In addition, it clearly indicates that online banking fraud incidents increased by 36% and ATM explosive attacks increased by 23% in 2022. Positive developments did occur, though, as evidenced by a 9 % decrease in reported mobile banking fraud incidents and a 17% decrease in fraudulent applications for vehicle asset finance.

South Africa has made strides in increasing access to financial banking as shown by the fact that more people own bank accounts currently, even though, active usage is still low. More than 81% of South Africans over the age of 16 had access to a bank account in 2021 (SABRIC, 2021:np). The low account utilisation levels are indicative of the fact that genuine access to financial services is still limited. Marakalala (2023:20) claims that the biggest banks controlled more than 85% of all deposits in 2020 despite an increase in new players. According to the Auditor General South Africa [AGSA] (2018:np) innovations from new entrant banks, such as technologically advanced start-ups, as well as the increased number of merchants providing financial services, including credit products introduced competition that compelled the traditional banking industry to undergo change. For example, changes effected as a result of competition from new entrant banks forced their competitors to reduce banking fees, introduce novel distribution models and introduce cutting-edge customer value propositions. Nedbank, FNB, ABSA, STD and Capitec are the newcomers that have made a big impact in the last four years. SABRIC also introduced new distribution models (like leveraging retail stores) and creative value propositions for customers, all of which have helped to lower banking fees (Marakalala, 2023:21).

The number of customers utilising online banking platforms and banking applications (Apps) to conduct transactions has increased as a result of the growing trend of digital implementation (Payments Association of South Africa, 2016:np). In an effort to decrease reliance on bank branches, banks have implemented next-generation Automated Teller Machines (ATM's), enhanced digital payment choices, and launched banking apps (AGSA, 2021:np). These measures enable clients to do a greater range of transactions. In the payments industry where many customers preferred to transact by means of cards rather than cash, the COVID-19 pandemic accelerated the rate at which businesses and consumers adopted technology transactions. For example, tap-and-go card transactions also experienced a significant increase (Annalise, 2022:20). These included removing the banking fees temporarily and enabling users to take out free cash from any ATM (Pieter, 2022:np).

1.3 PROBLEM STATEMENT

SABRIC annual reports from 2018/2022 emphasised that mobile fraud involves criminals targeting mobiles of bank customers who use banking applications (Apps) and Sim-Swaps. The prerequisite that mobile networks must o gather biometric data does not adequately address mobile fraud in SABI. Annual reports which analysed key targets identified the beneficiaries of an unauthorised debit order scam which led to their arrest. SABRIC released its first statistics on crime involving digital banking in 2019 (International Criminal Police Organisation [INTERPOL], 2020:np).

The report showed a marked increase in financial crime associated with nearly R3.3 billion in losses. According to SABRIC (2019:np), financial crime includes contact crimes, card fraud, and digital fraud, and they hinder economic advancement in South Africa. Fraud involving digital banking has increased by 45%, associated with a 47% increase in financial losses and the highest increase recorded in cybercrime. ACFE (2021:np) indicates that fraud involving banking applications has become the most significant threat, accounting for 60% of all incidents linked to digital banking; and soaring by an astonishing 89% each year.

Lately, criminals employ advanced technologies such as generative AI to execute intricate fraud schemes, including deepfake media and fraudulent emails (SABRIC, 2021:np). Amongst contact crimes, card fraud remains a significant challenge, particularly in online transactions. Online transactions that involve Card Not Present (CNP) fraud represented 68% of overall fraud losses, marking a 19% rise from the previous year (ACFE, 2019:np). Another crime affecting clients and employees of banks was an 85% increase in robberies in bank branches (SABRIC, 2018:np). ATM attacks still have an impact on the banking industry, particularly in Gauteng, despite a minor 9% decrease in incidents (SABRIC, 2018:np). This type of crime persists, despite the implementation of the dye-stain security measure as offenders do not seem to be bothered by the stained money. Application fraud, which consists of deceitful financial product applications, has notably escalated. It is particularly significant that the quantity of reported vehicle asset finance fraud cases rose by more than 100% (Open Data Charter, 2018:np).

Although an ever-growing number of people in South Africa now own bank accounts, and the country has made great strides in increasing access to financial services, active usage is still low. More than 81% of South Africans aged above 16, owned a bank account in 2021 (SABRIC, 2021:np). However, low account utilisation levels indicate that genuine access to financial services is still limited. GSMA (2020:np) claims that the banking system is still very consolidated, with the biggest banks controlling over 85% of all deposits in 2020, even with the rise in new role players. According to AGSA (2022:np), the banking industry has been undertaking changes as a result of competition from recently formed banks, technologically advanced start-ups, and an increase in the number of merchants providing financial services, including credit products. Over the past four years, five newcomers, namely Nedbank, FNB, ABSA, STD and Capitec have made a substantial contribution to the reduction of banking fees, the introduction of novel distribution models (like leveraging retail stores) and the introduction of cutting-edge customer value propositions (INTERPOL, 2021:np).

The number of customers utilising online banking platforms and banking apps to conduct transactions has increased due to the growing trend of digital adoption (PASA, 2016:np). In an effort to decrease reliance on bank branches, banks have implemented next-generation Automated Teller Machines (ATMs), enhanced digital payment choices, and launched banking apps (Wewege & Thomsett, 2020:37). The statement by Hayashi (2012:17) indicates that these measures enable clients to do a greater range of transactions. The COVID-19 pandemic accelerated the rate at which businesses and consumers adopted technology for transactions. Tap-and-go card transactions also experienced a significant increase (Annalise, 2022:20). New services included removing banking fees temporarily and enabling users to withdraw cash at no fee from any ATM (Pieter, 2022:np). Banking experts or investigators are aware that criminals have been using internet platforms since the advent of technology (Button and Cross, 2017:11).

SABRIC annual reports from 2018/2022 show that there were 13 438 incidents involving mobile phones to commit financial fraud online, and on banking apps that resulted in gross losses (over R250,000,000) for the industry (Pieter, 2022:np). In South Africa, digital banking through apps, websites, and phone calls now outperforms all traditional channels for transactional banking and is regarded as the safest. The aggregate number of digital banking fraud cases fell by 18% between 2020 and 2021 (AGSA, 2021:np). Total gross losses in digital banking during the reporting period increased by 45%, despite a decrease in the number of incidents (PASA, 2016:np).

Table 1.1: Mobile Fraud Allegations from 2018-2022

Allegations	**Type of Mobile Fraud**	Year	**Amount**
Incidents	SIM-Swap fraud	2018/2022	R13,438,00
Loss	Mobile banking fraud	2018/2022	R250,000,000
SIM Swap incidents	Banking apps fraud	2018/2022	R453.000.000
Mobile fraud Percentages	Debit card fraud	2018/2022	22%

Source: (SABRIC Report, 2021:np)

The mobile banking has made it easier for bank customers to manage their finances online used digital banking. However, this convenience comes with a risk. Kidnappers are now targeting bank accounts, using mobile phones to gather penetrating information and demand ransom (SABRIC, 2021:np). To make matters worse, refunds from banks aren't guaranteed, leaving victims with little to no recourse in the event of a financial loss. As a banking customer, it's essential to know how to protect yourself from these threats. cautions bank customers about safeguarding their mobile devices, especially in the light of emerging trends in crime such as app kidnapping, which has connections to both commercial and financial fraudsters (ACFE, 2022:np). Although mobile phone syndicates are not a new phenomenon, the SABRIC annual report 2018/2022 indicated a rising trend in which thieves steal mobile phones from their owners, giving criminals access to private and even confidential information that they can use to perpetrate crimes. The banks routinely tell their clients that they will never send them an email or SMS requesting that they click on a link that would take them to a website where they would have to verify or update their online banking details. Even with these guarantees and cautions, some clients succumb to these deceptions (PASA, 2016:np).

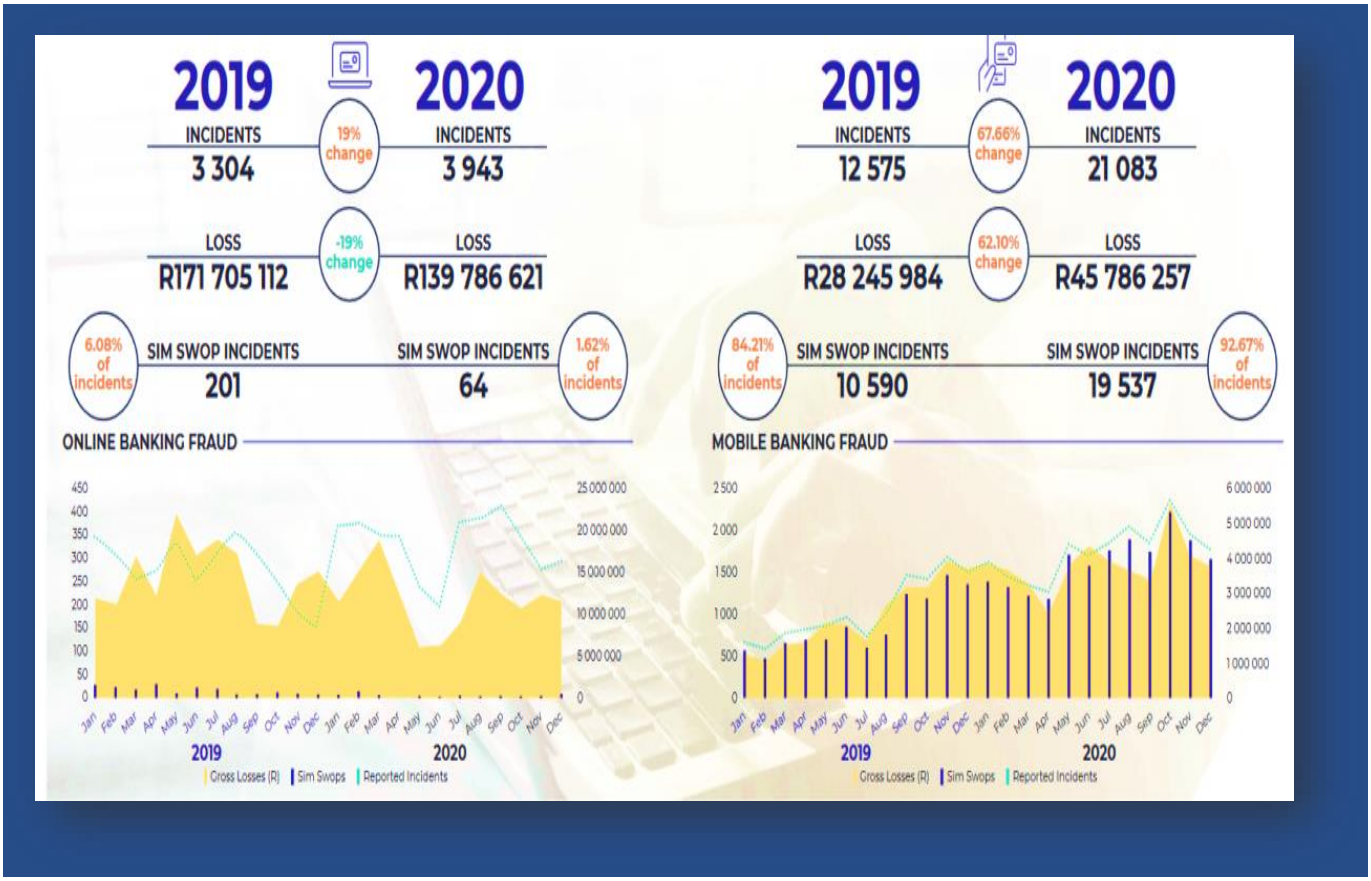
The statement by SABRIC (2021:np) indicated that there were weaknesses in the online banking payment process that fraudsters may take advantage of, particularly through mobile fraud. Banks responded to it by implementing a computer-based security system designed to assist in preventing mobile fraud. Priezkalns (2019:54) indicates that cyber-fraud is a relatively new crime that involves hackers obtaining personal data and using it for illicit purposes to access people's credit card and bank account details (AFCE, 2020:np) According to the Internet Service Providers Association [ISPA], (2020:np) unethical behaviour and fraud can be compared to economies that go through cycles, with frauds emerging as large explosions as booms shift to busts. In SABRIC, mobile fraud is pervasive, and among the growing threats to enterprises and governments (Girard, 2021:45; Marakalala, 2023:23). According to Buckles (2017:76) mobile fraud is still the main and most enduring threat that SABRIC faces.

Similar to this, the risk of mobile fraud in connection to ethics and good governance is described in the SABRIC annual report from 2028/2022 on SABRIC audits. One of the trickier frauds to investigate is mobile fraud. According to PricewaterhouseCoopers [PwC] (2022:np) the act of perpetration was either carried out by singular persons or by coordinated efforts between several individuals or organisations. SABRIC (2021:np) argues that mobile fraud in SABRIC has a negative impact on banking sectors.

To combat mobile fraud, the South African government primarily uses a framework for digital forensics and investigations that has been strengthened, statutory investigative bodies that have been established, and public anti-corruption campaigns that have been launched, appealing to the integrity of all people, especially those who are frequently hard to detect and investigate (Global System for Mobile

Communications Association [GSMCA], 2022:np). A growing challenge for the digital forensic process of identification is the likeness of internet enabled physical objects to their ordinary counterparts (Auditor-General of South Africa [AGSA], 2022:np).

Figure 1.1: Irregularities of a Biometrics-Based Solution to Combat Mobile Fraud



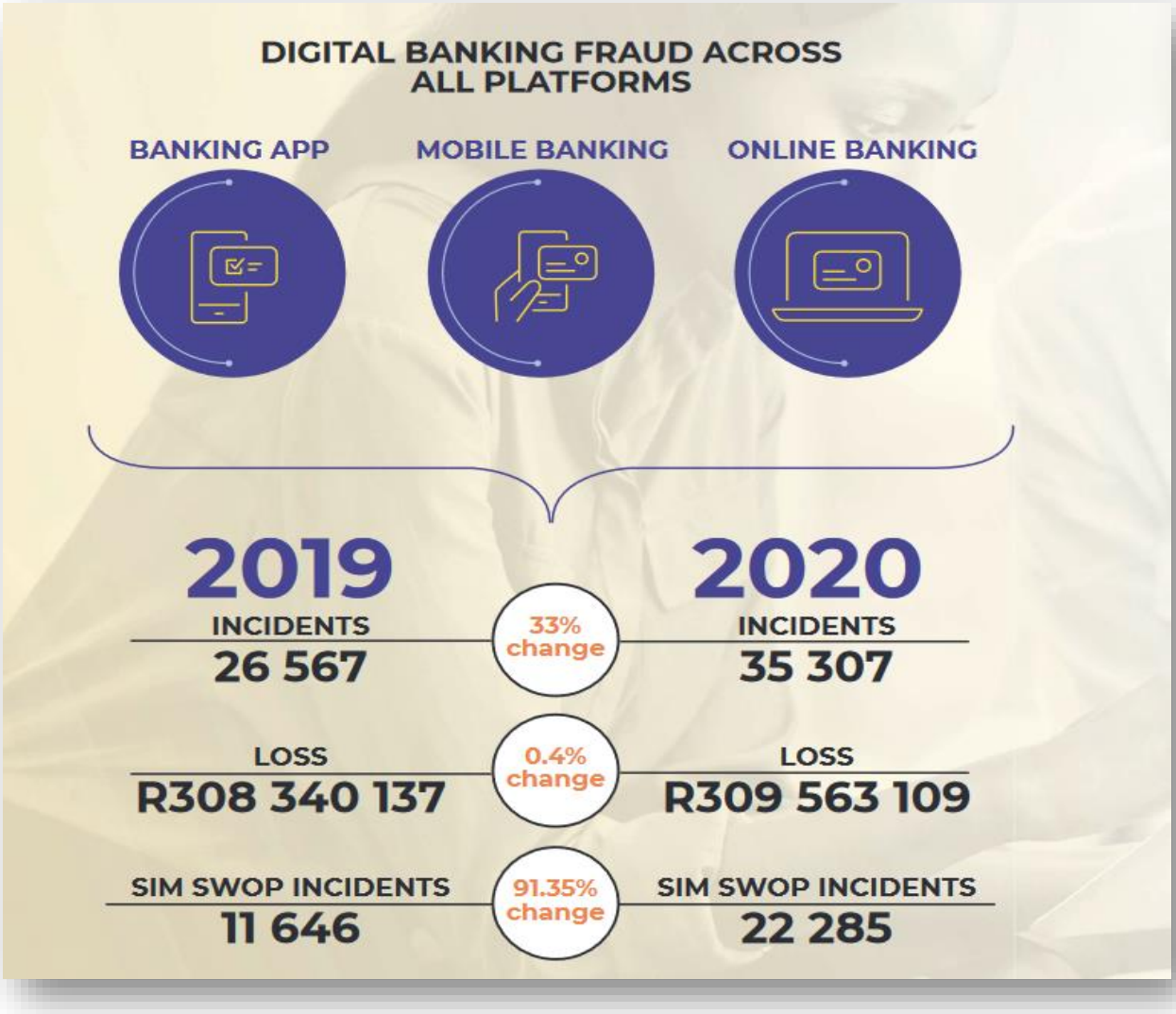
Source: (SABRIC Annual Report, 2021:np)

While fraud through online channels only makes up 1.1 % of recorded cases of digital banking crime, it accounts for the largest portion of gross losses (45.1%) of all types of fraud (SABRIC, 2021:np). Criminals often use phishing to trick bank clients into disclosing their personal information like usernames, passwords, credit card details and mobile phone numbers. According to Shulzhenko and Romashkin (2020:164), criminals sometimes also request the OTP that will be sent to a mobile phone when transacting. Concerns over the sharp increase in mobile fraud are shared by banks, mobile network operators and cell phone users (Coppolino, D'Antonio, Formicola, Massei & Romano, 2015b; AGSA, 2018:np). Phishing employs emails to trick users into entering their login credentials by taking them to a "spoofed" website that is designed to look authentic (ACFE, 2019:np).

Some believe that the practice of "vishing," which involves con artists posing as bank representatives and phoning prospective victims, increased dramatically in 2020. Vishing is employed by criminals who gain access to a victim's account as an extra step to trick the victim into giving them the necessary verification (SABRIC, 2018:np). SABRIC reports revealed that 92.7% (19,537) of mobile banking fraud incidents recorded in 2020 were SIM swaps which remain the most common. The increased ability of criminals to carry out SIM swaps may account for the significant increase in incidents (67.6%) and gross losses (62.1%) (SABRIC, 2022:np). According to INTERPOL (2020:np) fraud was another biometric-based option that was frequently discussed on the mobile banking channel. In this type of fraud, a family member or co-worker who knows the victim well and is in close proximity to him/her and his/her device, would gain access to the device and use the mobile banking platform to conduct transactions without the victim's knowledge (Kruse, 2015:54). Using quick cash sending services and buying airtime or electricity are two common behaviours that constitute cash-out methods. Online banking fraud has increased by 33% in the year 2022 (Marakalala, 2023:25).

Social engineering (phishing, vishing, and sim-swap) is the primary method of crime on this platform. In 2020, 92.7 % (19,537) of recorded cases of mobile banking fraud were carried out using this technique (SABRIC, 2018:np). When a login and password are used across several Apps and when they are saved elsewhere on a mobile device, fraudsters can obtain those credentials (AGSA, 2022:np). Phishing attacks have been around since the mid-1990s when they originally targeted emails. They are increasingly common on mobile devices and more advanced these days. Because mobile phishing attacks happen so frequently, Security Operations Centre (SOC) teams have more work to do to find out more about how to deal with the increasing threat of mobile phishing and keep reading (Gehl & Plecas, 2017:18).

Figure 1.2: Digital Banking Fraud



Source: (SABRIC Report, 2020:np)

As Figure 1.2 illustrates, debit card fraud increased by 22% in 2020, whereas credit card fraud declined by 7%, according to Figure 1.2. While the total ATM attacks decreased by 9%, ATM explosive events increased by 20% (SABRIC, 2018:np). Cybercriminals focused on this new way to victimise users, though, as the internet has become more mobile-friendly and people are using their phones more than ever before (for instance, banking sector clients use their smartphones for nearly 4.8 hours every day) (AGSA, 2019:np). Mobile phishing attacks may be harder to detect because they extend beyond regular email phishing. SMS-based attacks (smishing), malicious voice calls (vishing), and app-based phishing have exploded in popularity and severity (ISPA, 2021:np). Phishing relating to mobile fraud includes the following:

- ***Text messaging:*** phishing texts commonly impersonate banking apps or shipping providers.
- ***Voice mails****:* vishing attacks will mimic the IRS, loan providers, and more.
- ***Facebook Messenger:*** the perpetrators used links in messages.
- ***WhatsApp:*** attacks can target victims within the App and via email.

SABRIC (2019:np) indicates that the number of SABI digitally engaged customers rose by 10% to 3.5 million in the first half of the year. Because the company concentrated on promoting digital adoption throughout the portfolio, Standard Bank's digital transaction volumes rose by 15% (Pieter, 2022:np). In 2023, the bank's South African branch reported an average of 100 million monthly logins to its mobile app (Barker, 2018:75). According to SABRIC (2019:np), cybercriminals used the platforms that banking clients were using to carry out illegal activities, which had a significant effect on the banking sector. The Ombudsman for Banking Services [OBS] (2022:np) reports that a significant increase in the financial losses linked to digital banking fraud coincided with an increase in occurrences. According to AGSA (2019:np), gross losses increased from R440 million in 2021 to R740.8 million in 2022, indicating a 68% increase in the financial impact.

1.4 RESEARCH AIM AND OBJECTIVES OF THE STUDY

1.4.1 Research Aim

According to Kumar (2020:34), the phrases "goal," "purpose," "objective," and "aim" are frequently used synonymously. A research aim outlines the objectives, goals, and outcomes that a researcher hopes to accomplish during their investigation (Leedy & Ormrod, 2010:44; Creswell, 2020:88). Accordingly, a one goal of this particular study was to suggest a biometrics-based method for thwarting mobile fraud and while another goal was to pinpoint the precise problems that the research suggests solving to fulfil the study's goal (Kumar, 2020:15). The goal of a research study, according to Welman, Kruger and Mitchell (2011:02) is to examine the many types of research methodologies that are employed in the investigation.

- This study aims to explore a biometric-based solution to combat mobile fraud.

1.4.2 Research Objectives

To assist in realising this distinct vision, Maxfield and Babbie (2018:19) provide a list of five different types of research aims, including empowerment, description, explanation, and inquiry. Depoy and Gitlin (2016: 53) define research as an intentional, goal-directed, purposeful action carried out for a specified reason, such as (i) answering a specific question or query, (ii) solving a problem, or (iii)

addressing a specific argument or topic. Denscombe (2012:98); Kumar (2021:65) asserts that it is common to draw a line between research, best practice development, analysis and criticism, and empowerment of others. After considering the aforementioned concepts, the researcher determined that the objectives of the study are:

- To identify the prevalence of mobile fraud in the SABI;
- To identify factors contributing to mobile fraud in the SABI;
- To identify the challenges encountered by the forensic investigators in the investigation of mobile fraud in the SABI;
- To establish the best practices by developing a conceptual model to combat mobile fraud in the SABI.

1.5 RESEARCH QUESTION

Creswell (2020:18) states that the research question is the focal point of an entire study and dictates the kind of research, the design of the study, the methodology, the creation of the sample, as well as the methods for gathering and analysing data in the manner in which the findings are presented. Research questions offer the necessary clarification, guidance and specifics about the subject matter to be studied (Kumar, 2021:65). According to Denscombe (2012:73), a research question directs the investigation in a certain way. Furthermore, the author opines that a research question must fulfil three criteria: the fundamental concerns of the research, to be precise and specific, and to be exact regarding the kind of data that will be collected (Yin, 2018:45).

However, Kumar (2021:68) cautions that research questions should not be confused with "data collection questions" or questions that appeared on schedules. Determining the problem and then defining it into particular research questions that are pertinent to the subject under investigation is a crucial step in any scientific research project (Creswell, 2014:139). When conducting research on the specific issue that is the focus of the investigation, research questions are intended to clarify in advance what the researcher is examining (Gray, 2019:32).

A research question is raised when a researcher lacks sufficient understanding about the topic or problem being studied. Furthermore, the research question offers direction for the data collection necessary to address the issue that a study has identified.

This results in a targeted examination and interpretation of the information obtained from the literature review, the SABRIC annual statistical reports-2018/2022, the narrative literature review, and other pertinent sources (Ferguson, 2017:66).

To adhere to the above-mentioned authors, the researcher focused on the following research questions:

- What is the prevalence of mobile fraud in the SABI?
- What are the factors contributing to mobile fraud in the SABI?
- What are the challenges encountered by the forensic investigators when investigating mobile fraud in the SABI?
- What are the best practices by developing a conceptual model to combat mobile fraud in the SABI?

1.6 DEFINITION OF KEY CONCEPTS

The notions that recur throughout the entire research study are known as important theoretical concepts, since each subject has its unique jargon and ideas that are well-known to professionals within each discipline. The specific terminology and concepts should be clearly defined within the context of the chosen research models to achieve complete comprehension (Leedy & Ormrod, 2010:58). Clarifying important concepts is crucial because it puts research in the perspective of the field under investigation, which aids in the reader's understanding of the work (Creswell, 2020:34). The contextualisation of concepts helps readers learn more about the topic and improve their comprehension of the phenomenon under study (Babbie & Mouton, 2012:111; Maree, 2017:15; Kumar, 2021:62). The basic concepts discussed below were addressed in this study.

1.6.1 Biometric-Based Solution

Ashbourn (2014:27) explains that a person's identity can be verified or identified by means of biometrics and kept in a database is utilised in identification techniques. Authentication techniques are employed to verify a person's stated identification; in this instance, only stored biometric traits that match the claimed identity are compared (Jain, Deb and Engelsma, 2021:16). Biometric-based systems evaluate users live biological features (e.g., face shape, fingerprints, typing patterns) to authenticate their identities (Gray, 2014:39). The biometrics-based solution is the most efficient way to identify and authenticate individuals swiftly and accurately, based on their unique biological characteristics (Ashbourn, 2014:77).

1.6.2 Mobile Fraud

According to Davis and Pesch (2013:470), mobile fraud is characterised as a digital financial service where a person utilises a mobile phone handset to access a financial service or begin a financial transaction. Thus, Mobile Fraud Services (MFS) could involve checking balances, holding and transferring funds, and using mobile devices to make payments (ACFE, 2018:np), a financial transaction via a mobile phone device (INTERPOL, 2021:np). Thus, checking balances, storing and transferring funds, and making payments via mobile devices are examples of MFS. Therefore, regardless of any particular deployment architecture or transaction type, the phrase "mobile fraud" simply refers to using a mobile device to access financial services.

1.6.3 Fraud

According to the ACFE (2023:np), fraud refer to any international or deliberate act to deprive another of property or money by guile, deception, or other unfair means. Fraud is the unlawful and intentional creation of a deception that could be harmful to another party. Fraud is the deliberate use of deception to get something unfairly or illegally (Wells, 2017:44). Commonly, the term "fraud" refers to a variety of illegal actions, including bribery, extortion, embezzlement, conspiracy, theft, and corruption. The legal definition has been different in each jurisdiction since the Fraud Act was introduced in 2016. In most countries, committing fraud can be classified as a civil or criminal offence. Although the primary motivation for fraud is the desire to receive rewards of value, it can also occur with the specific intention of deceiving another individual or entity. For example, depending on the circumstances, making false claims could be considered fraud (Turvey and Crowder, 2017:23)

1.6.4 Mobile

According to Pieter (2022:np), digital technology refers to or mentions a mobile phone, typically one that may be used for computing, or a wireless, portable computer that is held in the hand, such as a mobile tablet, Public Display of Affection (PDA) or a mobile app.

1.6.5 Forensic Investigation

Turvey *et al.,* (2017:36) defines forensic investigation as an exhaustive, methodical search for the truth through the application of specialised skills, expert knowledge, and scientific methods and techniques in criminal conduct, civil matters, or administrative matters. According to Brandl (2017:31) forensic investigations are scientific processes that gather, examine, and evaluate evidence to establish facts and reconstruct events for investigative or legal purposes. All physical evidence related to a crime is

gathered and examined as part of forensic investigation in order to draw conclusions about a suspect (Kruse, 2015:19).

1.6.6 Combat

According to Henriksen (2007:210), the word ‘combat’ refers to fighting between two groups of armed forces. When you engage in combat, typically this means you engage in a fight that involves weapons. Combat emphasises the forceful or pressing opposition to something, even if all of these terms indicate ‘to put oneself against someone or something’. A combat is a battle, or a fight between two people. If people in authority combat something, they try to stop it happening (Button *et al.,* 2017:13).

1.6.7 SIM Swap Fraud

Phishing scams, such as SIM switch fraud, include con artists using phone emails or phone calls to obtain bank account information. ACFE (2023:np) indicates that in order to fool customers into disclosing personal information like verification numbers or one-time pins, con artists impersonate banks or mobile network providers. Social media is frequently used to obtain additional consumer information, such as the full name, birthdate, or any other information that allows con artists to pretend to be their victims (Shulzhenko *et al.,* 2020:169). After obtaining this data, con artists might pretend to be their victims and convince mobile network providers to reset or cancel the victim's SIM card. The fraudster then receives all calls and texts sent to the victim's phone, including passwords required to make bank transactions. This allows bank account scammers complete access to their victim's funds (Button *et al.,* 2017:16).

1.6.8 Digital Banking Fraud

Fraud aimed at online or mobile banking systems is known as digital banking fraud. It includes a variety of dishonest activities, including identity theft, breaking into accounts without authorisation, and conducting fraudulent transactions (Shulzhenko *et al.,* 2020:170). Cybercriminals and hackers employ various techniques, such as social engineering, malware, and phishing, to perpetrate fraudulent activities related to digital banking (ACFE, 2022:np). Fraudsters are using increasingly more complex techniques as digital banking gains popularity, making it harder for banks and their clients to spot and stop fraudulent activity (Al-Ghamdi, 2023:37).

1.7 VALUE OF THE STUDY

The financial industry, as well as future creativity and innovation, is seriously threatened by mobile fraud and related crimes (Gray, 2014:98). This study identifies areas that need more research, and which would contribute to the effectiveness and efficiency of the country's mobile fraud investigation. In addition to academics and academic institutions, the following implications of the study's findings would be beneficial to the entire corporate sector, the Criminal Justice System (CJS) and the global community.

1.7.1 Value for the Academia

Incidents of mobile fraud represent a serious risk to future innovation and creativity at SABRIC. This report clearly indicates areas that need more investigation and contributes to the effectiveness and efficiency of the country's mobile fraud investigation. In addition to academics and academic institutions, the researcher anticipates that the following benefits will come from the study's results for the CJS, the global community, and the entire corporate sector. The narrative literature review encompasses a variety of topics, including international instruments relevant to online mobile fraud, South African mobile fraud legislation, other nations, and the development of forensic investigation to combat mobile fraud, using biometric-based solutions in the banking industry in South Africa. The paper outlines several forensic investigation methods as well as the functions of various parties involved in the fight against mobile fraud. Additionally, it offers biometric-based ways to fight mobile fraud. It also accentuates the gaps that exist at the moment in the forensic examination of mobile fraud (Jain *et al., 2*021:56). Researchers, postgraduate students, and other academics worldwide could benefit from the numerous data collection and analysis methods employed in this study. It might help researchers to understand the value of forensic investigation and be aware of the factors that increase the likelihood of mobile fraud in order to combat it with a biometric-based solution.

1.7.2 Value for the South African Banking Industry

The results of this study could be used by the business sector to compel the government to address factors that impede the effectiveness and efficiency of forensic investigation to combat mobile fraud with a biometric based solution. The business community in general would benefit from the study’s analysis of the best approaches in dealing with mobile fraud.

1.7.3 Value for the Law Enforcement

The findings of this study have implications for all those involved in the CJS. The Hawks, for example, might benefit from this research by using a biometric-based approach to stop mobile fraud committed by criminals in the country. The concept of utilising biometric-based solutions to prevent mobile fraud is one that experts in forensic investigation at SABRIC would be more familiar with. This study identified barriers to the effective and successful prosecution of mobile crime and offers solutions. Policy makers, including legislators and bureaucrats, might gain more mobile knowledge and expertise which might assist in making informed decisions. This research might assist forensic investigators to understand the social and economic factors of the past and present that may have an impact on mobile fraudsters.

1.8 SUMMARY

This chapter served as an outline, in which the researcher described the SABRIC establishment, the three entities that make up mobile fraud, and the topic of investigating a biometric-based solution to combat mobile fraud in detail. The study's problem statement was explained, along with the research aim and objectives, essential concepts, and a brief explanation of the study's significance. Fraud is not unique to fast payments and has always existed in payment systems. Criminals constantly monitor how new technology and payment systems can be exploited and incorporate this information into their toolkits to attack account holders in a multitude of ways. This chapter explained the background of the study, problem statement, research aim and objectives, as well as the research questions. Furthermore, key concepts are defined, and the value of the study is highlighted.

CHAPTER TWO

RESEARCH METHODOLOGY AND DESIGN

2.1 INTRODUCTION

This chapter presents the research methodology followed in this study. It includes the philosophical worldview, the qualitative method that was adopted, the population and sampling procedure, data collection method, data analysis techniques and methods to ensure trustworthiness. A literature review offers a summary, interpretation, and critical analysis of prior studies on a particular subject while adhering to stringent methodological rules. It provides a comprehensive and flexible understanding of a research topic by integrating various viewpoints and sources. In contrast to systematic reviews, narrative literature reviews give priority to a thorough and critical summary, frequently emphasising the author's perspective and ideas. It is also crucial that the researcher conducts research in accordance with accepted standards. In this study the researcher adhered to ethical principles, as will be discussed in this chapter.

2.2 RESEARCH APPROACH

According to Creswell (2020:66); Kumar (2021:45) a research approach constitutes the framework for carrying out research. Furthermore, distinguishes an approach from a research design. To this end, the outlines approach as the basic rules for data collection, analysis and interpretation in pursuit of responding to a research question, whilst the research design refers to the blueprint or strategy how the approach is operationalised (Babbie & Mouton 2012:10). The problem investigated in this study, namely combating mobile fraud using biometric-based solutions, therefore forms the foundation of the design of choice (Leedy & Ormrod, 2016:26). The approach adopted in this study was qualitative. Qualitative research refers to an inquiry that seeks to understand phenomena through non-numerical data (Ary, Cheser, Sorensen & Walker, 2019; Creswell, 2020; Kumar, 2021). The approach thus draws from empirical sources that include persons directly involved with phenomena being studied, artefacts, literature, or any other materials that constitute the subject of the research question (Leedy & Ormrod, 2016:26). Sukhera (2022:415) emphasises that, unlike systematic reviews, narrative literature reviews prioritise a comprehensive and critical overview, often highlighting the author's interpretation and insights.

- ***Qualitative Synthesis:*** In contrast to meta-analysis or quantitative data analysis, literature reviews emphasis synthesising and interpreting the existing body of knowledge qualitatively.
- ***Flexibility and Depth:*** Researchers provide versatility in the kinds of sources covered and the depth of analysis, enabling a more nuanced comprehension of the subject under investigation.
- ***Author's Perspective:*** Literature reviews frequently include the author's viewpoint and interpretation of the literature, which can be both a benefit and a possible constraint.
- ***Exploratory Approach:*** Literature reviews are especially helpful for providing a historical summary of a subject, finding gaps in the literature, or examining novel or under-researched topics.

Knowledge synthesis based on a particular research tradition is known as "narrative literature reviews". They are frequently portrayed as unsystematic, which suggests that narrative literature reviews rank lower in the evidence hierarchy than other review format (Ferrari, 2015:232. Narrative literature reviews, on the other hand, are really helpful to medical teachers and scholars. Sukhera (2022:417) indicates that narrative reviews may cover a wide range of studies and offer a comprehensive summary, complete with interpretation and critique. Conversely, a systematic review frequently concentrates on a single issue in a particular setting, using a pre-specified method to combine results from similar investigations (Greenhalgh, Thorne & Malterud, 2018:48). Some examples of narrative review kinds are integrative, critical, and state-of-the-art reviews, to name a few. While narrative literature reviews do not require a highly specific research question like systematic reviews, it is helpful to have a clear focus for the review:

- ***Search for Literature:*** A broad search strategy is employed to identify relevant scholarly articles, books, and other sources.
- ***Select and Synthesise:*** The selected literature is then read, summarised, interpreted, and critically evaluated, often drawing connections between different studies and perspectives.
- ***Identify Themes and Patterns:*** Narrative literature reviews often aim to identify key themes, trends, and patterns emerging from the literature.
- ***Develop a Narrative:*** The conclusions are then combined into a compelling and informative narrative that represents the current state of knowledge on the subject.

In the context of this study, the narrative literature review emanates from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, INTERPOL) and AGSA annual statistical reports from 2018/2022) which were perused and interpreted in relation to the research question which investigated mobile fraud. The study selected qualitative research as a method because interrogating these documents enabled the researcher to gain first-hand empirical knowledge on mobile fraud, a trait of qualitative research that is confirmed by Babbie (2021:77); Bertram & Christiansen (2014:34).

To operationalise the approach, the study used an exploratory design. Exploratory designs are used where little is known about the subject matter being researched. The choice of the design was purely determined by the fact that, very little is known about mobile fraud and the use of biometrics in combating or investigating this kind of problem in the South African banking sector context.

2.3 THE PHILOSOPHICAL WORLDVIEW

According to Creswell (2020:6), the philosophical worldview is crucial to research. When planning a study, researchers must consider the assumptions they bring to the study, the inquiry strategy that is connected to this worldview, and the particular research methods or procedures that put the approach into practice (Babbie & Mouton, 2021:66). There are various research worldviews, such as the pragmatic worldview, the advocacy/participatory worldview, the post-positivist worldview, and the social constructive worldview (Snyder, 2019:337; Kumar, 2020:45). The researcher conducted this investigation by means of the Social Constructive Worldview.

2.3.1 The worldviews

Post-positivist: This perspective places a strong emphasis on objectivity, the use of non-empirical data for literature studies, and the application of rigorous research methods to narrative literature reviews of mobile fraud. Leavy (2022:67) indicates that post-positivist research on banking subject matter reflects the need to pinpoint and investigate the factors that affect results (Creswell, 2020:13).

Constructivism: Creswell (2020:16) indicated that qualitative research techniques are used to investigate secondary data analysis viewpoints, as this worldview is centred on comprehending the significance of experiences and the social construction of knowledge.

Pragmatism: This problem-centred worldview employs a range of techniques to solve real-world issues and concentrates on the beneficial effects of decisions.

2.3.2 Distinctive Methods and Subtypes

It is typical to think of the narrative review as an umbrella phrase that encompasses a number of different review subcategories (Greenhalgh, *et al.,* 2018:55). Narrative sub-genres share the goal of increasing knowledge of a subject while also explaining the rationale behind a researcher's choice to investigate and analyse the subject in a certain manner. Narrative literature reviews come in a number of forms, employing diverse methods, each providing a different perspective on how to analyse and interpret the literature and address the research topic. The forthcoming SABRIC special articles on reviews will also discuss the popular narrative review kinds addressed in this thesis which are theory integration, critical, meta-ethnographic, and state-of-the-art reviews.

A ***state-of-the-art review*** strives to compile a study on a given subject along a timeline of keyshifts in knowledge orresearch approaches. State-of-the-art reviews concentrate on these turning points in the history of our changing understanding of phenomenon, providing a synopsis of the present state of knowledge, how that understanding was created, and a glimpse into potential future paths (Ferrari, 2015:234).

A ***meta-ethnographic review*** choosing and analysing qualitative information on a specific issue is part of a meta-ethnographic study. This sort of knowledge synthesis makes use of just qualitative data in an attempt to come to new understandings or conclusions about a topic (Greenhalgh *et al.,* 2018:69). It integrates qualitative research findings with analyses from past publications to produce new knowledge that encompasses these occasionally modest, individual studies.

A *meta-narrative review* aims to understand and analyse inconsistencies and contradictions in the literature. The meta-narrative review, which maps out the various interpretations of a particular topic, carries conducts a focused investigation to define and contrast stories, and then, as part of the analysis, seeks to understand how these stories are interpreted in different fields or historical contexts (Greenhalgh *et al.,* 2018:56).

A *critical review* using an interpretive lens, the review is a synthesis of literature: the review is shaped by a theory, a critical viewpoint, or viewpoints from other fields. areas for literary analysis guidance. According to Greenhalgh *et al.,* (2018:58), critical reviews use an interpretive method that combines the reviewer's theoretical framework with well-known theories and models in order to make things easier. the integration and analysis of data from several research investigations.

Reviewers first establish and describe their interpretive theoretical viewpoint, which is shaped by their own skills and experiences. Key themes pertaining to a research topic are then identified and collected through a partial search.

An ***integrative review*** generally takes one of two distinct orientations. Publications of evidence-based studies with different methodologies are analysed and synthesised by empirical integrative reviews. Conversely, theoretical integrative reviews analyse the available theories that address a phenomenon, offer a critique of those theories, and suggest a step forward in their development (Greenhalgh, *et al.,* 2018:62). Both kinds of integrative reviews adhere to a multistage process that includes identifying the problem, looking for it, evaluating it, analysing it, and presenting it.

As noted by Creswell (2020:16), the Social Constructivist Worldview is a viewpoint and is commonly regarded as a method for qualitative research. Additionally, Creswell explains that social constructivism is predicated on the idea that people try to comprehend the world in which they live and work. Exploring biometric-based solutions to combat mobile fraud at SABRIC and comprehending the theory and practical aspects of this application serve as the foundation for the desire to adopt a constructivist paradigm. In order to further investigate biometric-based solutions for preventing mobile fraud in the area under investigation, this will be explained in detail and will benefit SABRIC.

Qualitative research follows the anti-positivist worldview. The proponents of anti-positivism subscribe to the theoretical posture that postulates epistemology as the basis for research. This implies studying phenomena drawing from the lived experiences of persons involved with phenomena being studied, or from direct empirical sources that include literature, artefacts, paintings or any other materials that address the question of the research.

2.4 STUDY LOCATION

This is literature study (narrative literature reviews) and only literature related to the topic under investigation was perused to obtain in depth information regarding the commission of mobile fraud at SABRIC. Narrative literature reviews are a valuable tool for exploring, synthesising, and interpreting existing research, especially when a broad overview or nuanced understanding is needed. While they have limitations, they can provide valuable insights into a research area and contribute to the development of new knowledge and theories.

2.5 TARGET POPULATION AND SAMPLING

2.5.1 Study Population

The researcher targeted secondary data relevant to the study as sources of information. The data used were obtained from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, INTERPOL and AGSA annual statistical reports from 2018/2022 that were used to choose the sample referred to as the population and generalise the study's findings (David & Thomas, 2018:33; Creswell, 2020:29). The term universe refers to all subjects that have the characteristics that the researcher is interested in, for instance all people who live in the world and have obtained a post-graduate degree. Bertram *et al.,* (2014:59) and DePoy and Gitlin, (2016:90) posit that the word 'population' was used for narrative literature reviews and on statistic annual reports 2018/2022 that could be included in a study. It could also be objects, subjects, phenomena, the SABRIC annual report, events and activities that the researcher wishes to research to establish new knowledge. The annual statistical reports-2018/2022 made up the population of this study. In the opinion of Saunders, Lewis and Thornhill, 2019:86); Bachman and Schutt (2015:106) it is imperative for a researcher to establish the 'parent population' before defining any number of units of analysis. When a sample needs to be chosen, this would represent the entire population.

The above-mentioned writers contend that in order to determine the population for a research project, three important questions need to be addressed (Saunders *et al.,* 2017:87; Bachman *et al.,* 2015:112). The research question, which is outlined below, must provide the basis for these inquiries. They might affect the final result of the research if they are not appropriately accessed. The research questions, which are outlined below, must provide the basis for these inquiries. They might affect the final results if they are not appropriately accessed. The questions must:

- How does the specific sub-sets be applied on the population to be excluded because of the prevalence of certain scenarios or experiences?
- It must also be ascertained whether any additional sub-population needs to be included. The literature review discusses, and analyses published information from the annual statistical reports from 2018/2022 that are now available, and which have been determined to be the parent population for this qualitative research study. Official authorisation from SABRIC was obtained to do data analysis.

2.5.2 Sampling Procedures

In this study, an inquiry narrative literature review, selected from a population is referred to as a sample. Finding accurate information about the sample is the aim. It is up to the researcher g to choose how to monitor the annual statistical reports from 2018/2022. Sampling, which is utilised for data generation by any means, relates to the concepts and practices used to locate, select, and obtain access to pertinent units. The fundamental idea behind sampling is that reliable results can be obtained without having to obtain information from every member of the 'population' being surveyed (Denscombe, 2012:23). Non-probability sampling is a strategy in which the researcher chooses samples based on the researcher's subjective judgment rather than random selection. Probability sampling is used when the probability of the chosen population elements has not yet been defined. According to Denscombe (2012:23) and Bachman *et al.,* (2015:108) it is a less rigorous approach. Non-probability sampling was the method of choice for this study and was used extensively. According to Maree (2017:80) and Welman *et al.,* (2011:56) all authors mentioned before? non-probability sampling should be used instead of random selection when conducting research because it eliminates the need for random selection when selecting a research sample. Similarly, Hennink, Hutter and Bailey (2020:98) argue that non-probability sampling is aligned with qualitative research.

The foundational data for this research came from the narrative literature reviews (annual statistical reports-2018/2022) that were specifically related to mobile fraud. A five-year basis data set was purposefully chosen by the researcher using the following justification:

- To get an understanding of the past and current MO types perpetrated into mobile fraud at SABRIC and to determine similarities, if any;
- To align with the aim of this research and the research questions as defined, identified as crucial from an accuracy and completeness perspective for qualitative research.

2.6 DATA COLLECTION

The various strategies can be applied when gathering data by studying relevant literature, guides, records, observation guides and the literature study from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, as well as the INTERPOL and the AGSA annual statistical reports from 2018/2022. Bertram *et al.,* (2014:71); Creswell (2014:13) and Kumar (2020:76) highlighted that data provide the evidence or information that researchers gather to obtain answers to the specific questions they are posing.

Setting the parameters for the study, gathering data through literature study (annual statistical reports-2018/2022) and visual materials, and developing the procedure for documenting material are all included assert that gathering data is the aspect of a research study that takes the longest. This task must be completed because without data, it would be impossible to increase one's knowledge base, provide an explanation for the 'unknown', or add new information to that which already exists.

A narrative literature review was used in this study as the primary mode of data collection, by conducting a review on the annual reports from 2018/2022. According to Khaldi (2017:25) data collection is the methodical collection of facts and figures. The following factors as Kumar (2021:164) explicitly states, must be taken into consideration when choosing a specific research method for gathering data:

- The types of information collected;
- The purpose of data collection;
- The resources available;
- The skills and techniques of a particular method to collect data;
- The socioeconomic-demographic characteristics of the research study.

The fundamental goal of any research study is to obtain information in order to respond to the questions posed by the investigation (Leavy, 2022:87). According to Bryman (2012:12) the researcher designs research instruments to put what needs to be known into practice and determines in advance the general parameters of what needs to be learned. All the research literature that is currently available on a subject or topic is referred to as a literature review (Flick, 2020:76). Given the many advantages of conducting a thorough literature review, the researcher should ultimately be well-versed in the relevant literature (Leedy & Ormrod, 2016:51). Both domestic and foreign resources were consulted to gather information on the subject for the study. The Internet, Google Scholar, books, journals, articles, and dissertations were among the sources consulted, as well as the SABRIC annual statistical reports, ACFE annual statistical reports, GSMA, ISPA and the AGSA reports from 2018/2022 to analyse data. Additionally, the researcher used a variety of search engines on the World Wide Web (www) to help retrieve information from pertinent websites. In order to address the research questions and aim, multiple sources were consulted. According to Mason (2018:87), it is crucial to carry out a literature review to determine what has previously been accomplished in a particular field of study. According to preliminary results, there is information about the subject matter but not the particular subject of this investigation.

2.7 DATA ANALYSIS

Leedy and Ormrod (2016:32) stated that after having collected the data, that data must be prepared for data entry. According to De Vos *et al.,* (2011:252), data preparation includes checking and editing collected data and eventually coding it. Qualitative data analysis is a rigorous and logical process through which data are given meaning. The analysis of the data can lead to an initial description of the data. Then, through a process of disaggregating the data into smaller parts, it revealed how these connect into new concepts, providing the basis for a fresh description However, merely describing the data is not enough; there is a need to interpret, to understand and to (Bryman, 2021:76). Explain the data. According to Creswell (2014:179) data analysis in qualitative research consists of preparing and organising the data for analysis, then reducing the data into themes through a process of coding and condensing the codes, and finally representing the data in figures, tables or a discussion.

In this study, qualitative data were analysed using the thematic technique, in line with Creswell's data analysis spiral. Creswell (2014:182) The same author further explains that in thematic analyses, researchers engage in the process of moving in analytic circles rather than using a fixed linear approach. A researcher enters with data or text and exits with an account or a narrative. Leedy and Ormrod (2016:152) state that data analysis involves the categorisation of data according to its meaning and in which patterns, regularities and critical events are identified. The researcher transcribed narrative literature reviews, to facilitate the collection of information. Leedy and Ormrod (2016:153) provide a framework to be followed after the transcribing of narrative literature reviews, which this researcher followed:

Data organisation: The process begins with data management. Early on in the analysis process, researchers file their data. Physical folders and electronic documents were used to organise the raw data gathered from the literature review and the online narrative literature reviews for this study.

Reading and memoing: Before dividing the transcripts into smaller sections, researchers read each one multiples time to gain a sense of the entire database. Writing memos or notes during this preliminary data exploration phase is beneficial. The data in this study were subjected to multiple analyses to gain a comprehensive understanding of its components and to obtain a sense of the data as a whole. The researcher was able to take notes for initial interpretation during this process.

The process of characterising, categorising, and analysing data into themes is the main objective of this step: The foundation of analysing qualitative data is creating categories. In this step, scholars create thorough descriptions, formulate themes, and offer an interpretation based on their own opinions or viewpoints regarding the literature (Gray, 2014:65). In order to describe, categorise, and interpret the text, it must be combined into discrete informational groups. Moving past classification means dissecting the text to find themes or categories. Flick (2020:34) explains that in qualitative research, themes, also known as categories, are major informational units made up of multiple pieces combined to create a single concept. By grouping the data into categories and subcategories, this researcher was able to detect particular patterns in the data.

Data interpretation is the process of making sense of the data: The researcher used descriptions or themes to interpret the meaning inherent in the data.

Data visualisation and representation: In the last stage of the data analysis spiral, one displays the results. Instead of numbers, data contain text. The data were represented by the researcher using categories and subcategories.

Find statements that are relevant to the topic: The researcher did this to discern which information in the narrative literature reviews was pertinent and which was not and then divided the relevant information into brief sentences or segments that each represented a single, focused idea.

To achieve this, the researcher made sure that the sentences were categorised into groups that reflected the different meanings of the phenomenon as experienced in the annual reports (Khaldi, 2017:12). To do this, the researcher took into account the different ways that the SABRIC annual report addressed the narrative literature reviews.

Construct a Composite: After determining the different interpretations, the researcher created a general overview of the subject of the study (Kathryn, 2017:23). The narrative literature reviews, (SABRIC, ACFE, GSMA, ISPA, INTERPOL) and AGSA annual statistical reports from 2018/2022), were used.

In conclusion, the themes used by the researcher in this study significantly contributed to the identification and description of the biometric-based solutions to combat mobile fraud at SABRIC. The tapestry of information derived from the narrative literature review (Annual Statistical Report-2018/2022) offered a vibrant and vital insight into the biometric-based solutions to combat mobile fraud at SABRIC.

2.8 METHODS TO ENSURE TRUSTWORTHINESS

Although many qualitative researchers contend that the term ‘validity’ is not applicable to interpretive at research, they acknowledge the need for some sort of qualifying check on their work that addresses the question (Bertran & Christiansen, 2014:188).

2.8.1 Credibility

Credibility could be improved in a number of ways while gathering and analysing data. In certain instances, having two researchers watch the same thing at the same time say, in a classroom, might increase credibility (Maxfield, Babbie, & Schuck, 2011:476). As a result, the two can compare their experiences and lessons gained from studying the identical object and assess whether their outcomes differed (Bertram *et al.,* 2014:188). According to Marshall and Rossman (2016:19) credibility is a notion of trustworthiness that essentially equates to internal validity. The degree to which the gathered data accurately capture the many facts of the event is referred to as its credibility. Similar biometric technology questions are used in this study to fight mobile fraud in SABRIC. This was carried out to verify that they comprehended the issue that this investigation looked into. The investigator made certain that all of the chosen SABRIC annual statistical reports-2018/2022 and literature analyses followed the narrative literature reviews guide exactly.

2.8.2 Transferability

Mason (2018:66) argues that research can be undertaken to the prevalence that it applies to other situations with similar characteristics through transferability. The degree to which the findings of qualitative research can be applied to different circumstances needing further narrative literature reviews, or SABRIC annual statistical reports-2018/2022 is referred to as transferability (Anney, 2014:277). According to Morrow (2015:31); Babbie and Mouton (2021:88), transferability can be improved by using precise explanations of the research, participant perceptions and understandings, methodology, result interpretation, and peer debriefer input. Transferability is improved by knowledge of the researcher's role as a tool in the process and interactions with SABRIC annual statistical reports-2018/2022 or narrative literature reviews.

2.8.3 Dependability

According to Bertram *et al.,* (2014:190), a researcher might also try to improve dependability. This is a reference to the point at which the researcher is able to explain why there might be differences in this study, for instance, between cases.

It can also entail highlighting the key distinctions between this study and earlier research in the area. Anney (2014:278) regards dependability as the capacity of results to hold up over time. Morrow (2015:90) refers to dependability as the confirmation that the data represent the changing conditions of the phenomenon under study and should be consistent across time, researchers and analysis techniques. An additional person provides data confirmation by auditing the results and confirming that the Grounded Theory Methodology (GTM) protocols have been adhered to and correctly used (Brown*& Smith,* 2022:47). The audit trail, which contains a complete chronology of research activities and methods, can be examined by peer researchers, student advisers, or co-workers to assess the credibility of the findings (Morrow, 2015:21; Mukherjee, 2020:8).

2.8.4 Conformability

It is standard procedure to determine if multiple persons can confirm the same results. According to Bertram *et al.,* (2014:190), conformability could be improved by providing readers with enough information about the research process to determine whether they would have come to the same or a similar conclusion. Additionally, Anney (2014:279), regards conformability as the prevalence to which the findings of an investigation could be verified or validated by additional researchers. Although bracketing was followed in order to achieve accurate findings and prevent manipulation of facts collected from the narrative literature reviews, or the SABRIC annual statistical reports-2018/2022 selected for this study, the researcher may have his own opinions regarding the research issue to be researched.

2.9 ETHICAL CONSIDERATIONS

Nayab (2020:27) highlighted that as the study of moral value systems and good conduct principles. Behaviour that complies with widely recognised moral standards is considered ethical. Research ethics pertains to the morality and propriety of performing research. The established norms and values should guide the right and wrong of scientific research Saunders *et al.,* 2019:111). It should be morally permissible to perform research activities in this way. According to Noble and Smith (2015:90), performing research in a way that is ordinarily and legally correct is the definition of ethics. The following were the measures put in place to ensure that this study subscribes to ethics in science:

- *Non-plagiarism:* All sources used were acknowledged in-text and in the list of references. No information from any source was copied *verbatim*.
- *Non-bias:* The researcher engaged with literature (units of analysis) in a fair manner, without drawing illogical or unreasonable assumptions.

- *Honest reporting:* The researcher ensured that information reported in the findings and conclusions of the study reflect the spirit and letter of all sources/analytical units used in the study.
- *Ethical clearance:* The study obtained ethical clearance from the university (see Annexure B).

2.10 SUMMARY

The research design and technique employed are emphasised in this chapter by outlining the target population, sampling techniques, study location, research design, adopted research approach, data collection, and analytic methods. Also described in the chapter are details about ethical considerations and the philosophical framework that the researcher used for the investigation. Literature reviews provide a readable, thoughtful, and practical synthesis on a topic. They allow review authors to advance new ideas while describing and interpreting literature in the field. Narrative literature reviews do not aim to be systematic syntheses that answer a specific, highly focused question; instead, they offer carefully thought out and rigorous interpretations of a body of knowledge. Such reviews will not provide an exhaustive, comprehensive review of the literature; however, they are useful for a rich and meaningful summary of a topic.

CHAPTER THREE

THE PREVALENCE OF MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

3.1 INTRODUCTION

This chapter presents the discussion on the prevalence of mobile fraud in the SABRIC. This is followed by a discussion aimed at providing an overview of mobile fraud at SABRIC, including the forms of fraud and the techniques used in the commission of mobile fraud. Furthermore, the chapter presents the legislative framework regulating the banking industry. The techniques used in the commission of mobile fraud were discussed.

3.2 AN OVERVIEW OF MOBILE FRAUD IN THE SABI

The annual statistical reports from 2018/2022 observed a slight rise in the incidence of SIM swap fraud, which suggests that mobile service providers need to improve their data security to safeguard clients against scammers using false identities and SIM swapping tactics (SABRIC, 2022:np). In South Africa, scammers took advantage of weaknesses in the handling of sensitive data, employed various social engineering methods to acquire the private information of their targets, and succeeded in accessing usernames and passwords saved on numerous devices or applications. Scammers often employ fishing to contact victims pretending to be bank personnel or service providers. Wells (2017:66) highlighted that criminal coerced victim into revealing confidential information through the use of social engineering techniques, which was subsequently utilised for fraudulent purposes.

A key part of their strategy involved intercepting transactional verification tokens, such as OTPs, Random Verification Numbers (RVN), and transaction approval requests (SABRIC, 2018:np). Fraudsters succeeded to achieve this by convincing victims to approve transactions or provide verification numbers during the call. According to SABRIC annual reports (2022:np), there were only 71 SIM swap incidents in 2022, compared to 4,508 cases in 2021. The number of cases in which people have been abducted or hijacked under duress to obtain unauthorised access to their banking applications has increased (INTERPOL, 2020:np). The use of physical force or threats to coerce victims into opening their banking applications and starting money transfers makes this criminal activity a worrying trend (Wells (2017:72). However, it is crucial to remember that there have not been any reports of a verified compromise of banking apps up to this point.

INTERPOL (2020:np) states that barcoded identification documents, Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) or Financial Intelligence Centre Act (FICA) information, a facial image will be validated and returned to the Department of Home Affairs. This avoids identity fraud and demonstrates that the person requesting for services online is a 'real' person, not a deepfake. SIM swaps are no longer necessary because all SIM cards are now data connected to a valid individual with exact RICA requirements (SABRIC, 2022:np). Kruse (2015:94) indicates that several mobile fraud cases were classified and influenced by various categories, such as revenue loss and fraudulent cash disbursement (expenditures), as well as biometric-based solutions for combating mobile fraud at SABRIC. This study also emphasised that the common detection methods were characterised by the change in the biometric-based solution in combating mobile fraud at SABRIC, which included both external and internal employees (Brytting *et al.,* 2019:99). Mobile fraud is a complex issue that encompasses a wide range of illegal behaviours, from bid rigging during the pre-contract award stage to fake billing during the post-contract award phase. It could be committed by both internal and external parties (INTERPOL, 2020:np).

According to the SABRIC annual reports (2018/2022), mobile fraud is difficult to detect, and such occurrences are rarely reported. As a result, it is impossible to assess the scope of the problem. Furthermore, when mobile fraud is found, the necessary resources are directed toward analysing documents to indicate mobile fraud or irregularity and looking for commonalities particular to combating mobile fraud at SABRIC (SABRIC, 2020:np). According to Labuschagne (2015:53), *modus operandi* is a method of identifying mobile fraud that can alter over time. The identification of mobile fraud is dependent on the collection of evidence material to ascertain the *modus operandi* and, perhaps, the name of the perpetrator, which stays at the forefront of the SABRIC annual report in mobile fraud.

Furthermore, this chapter focuses on the biometric-based solutions for combating mobile fraud at SABRIC. According to statistics from the Southern African Fraud Prevention Service (SAFPS), there was a 600% rise in fraud incidents reported by its members in 2022 compared to 2018. The SAFPS website allows customers to report fraud or other questionable conduct. This suspicious activity includes occasions where customers obtain phone banking information, as well as a false or suspicious looking online purchasing website/portal (Button *et al.,* 2017:18). These reports are compiled and provided to law enforcement for inquiry. Users are also given a scam hotline number to call when reporting a fraudulent event to their banks, retailers, or insurance organisations (Button *et al.,* 2017:21).

Therefore, instead of searching for each institution's phone number online, customers will only need to remember one (ACFE, 2022:np). Contextual mobile fraud happens when fraudulent activities take place

specifically on mobile platforms or devices (INTERPOL, 2021:np). This kind of fraud exploits the particular qualities and weaknesses of mobile devices and operating systems. The proliferation of smartphones and mobile applications has provided new opportunities for fraudsters to exploit numerous flaws and vulnerabilities (Brytting, Minogue, & Morino, 2019:97).

It is usually very easy for a fraudster to utilise customers previously installed remote access solutions (such as TeamViewer) to transfer all of the client's personal files and data (ACFE, 2022:np). Fraud continues to rise in the absence of adequate corporate anti-fraud procedures and common user knowledge. Fraudsters utilise dark web marketplaces and forums to actively discuss, plan, and share tools aimed at mobile users. Consequently, it is very dangerous to ignore the threat (Button *et al.,* 2017:27).

Mobile fraud has become a major threat as consumers rely more on smartphones for activities such as online banking, shopping, and social interactions (Brytting *et al.,* 2019:109). Fraud occurs when someone purposefully causes financial harm to another individual through deception. The fraudster usually accomplishes this by deceiving the victim to seize control of their possessions. During the early COVID -19 pandemic lockdowns, people and companies naturally moved online to maintain their banking services (INTERPOL, 2020:np). This massive surge of new online customers includes brick-and-mortar stores, forcing them to create an e-commerce platform in order to survive. Existing online businesses seek to entice users with m-commerce platforms and more alternative payment choices. Subsequently, mobile banking, which was already popular prior to the epidemic, saw a significant increase in use (ACFE, 2022:np).

As a result, global payments and transactions increased dramatically, ensuring continuous business revenue growth (Wells, 2015:25). Unfortunately, this surge coincided with an increase in global fraud rates, as fraudsters targeted people who were unaware of online hazards or had insufficient anti-fraud and security measures in place. Because of this lack of understanding, fraudsters resorted to tried-and-true methods of defrauding victims, the majority of which rely on establishing confidence and having victims perform half the work. Fraud is typically defined as dishonesty with the intent to gain an unfair or unlawful advantage (SABRIC, 2018:np). Fraud in the context of mobile fraud is defined as the intentional and deliberate action taken by players in the mobile financial services eco-system with the goal of gaining profit (in cash or e-money), denying other players revenue, and/or damaging the reputation of other stakeholders (Button *et al.,* 2017:29). According to INTERPOL (2020:np) a user's mobile fraud identity becomes a natural target for criminals because most banks today use their customers' mobile phones as another way (second factor) to identify and authorise credit card, ATM, point-of-sale or Internet banking transactions.

3.2.1 Forms of mobile fraud

Mobile fraud takes several forms, which include:

Malware: Malicious malware can be disguised as legal mobile applications or integrated into web sites, infecting devices and collecting sensitive information like passwords, credit card numbers, and personal data (Dunham, 2008:76).

Phishing: Fraudsters send communications or emails that appear to be from legitimate sources, tricking users into providing personal information or conducting illicit transactions (INTERPOL, 2020:np).

SMS fraud: Scammers send bogus SMS texts containing fake offers, contest winners, or urgent requests for personal information in order to trick consumers into giving sensitive data or subscribing to pricey premium services (Button *et al.,* 2017:38).

Fake apps Fraudster's design apps that seem like famous services or games to fool consumers into downloading counterfeit mobile applications. These bogus apps can acquire user data or engage in fraudulent activities such as unauthorised in-app purchases of suggestions (INTERPOL, 2020:np).

Click fraud: Fraudsters create phone clicks on mobile ads to increase the number of impressions or clicks, increasing advertising expenses for advertisers while giving no genuine benefit.

SIM card swapping: Attackers persuade mobile service providers to switch a victim's phone number to a new SIM card that they then control. This enables them to get access to the victim's accounts, conduct fraudulent activities, and obtain sensitive information (ACFE, 2020:np).

The statement by SABRIC (2020:np) indicates that investigating the relationships of unresolved cases involves an inquiry into the biometric approach for tackling mobile fraud with SABRIC. Data collection is utilised to reveal the tactics of criminals in mobile fraud scenarios that have not been resolved. There is a regular comparison of arrest strategies to the investigation of ongoing cases (Button *et al.,* 2017:41). By gathering strategic intelligence, investigators can generate leads and pinpoint suspects in active cases, focusing on prioritising and eliminating offenders and addressing ongoing mobile fraud occurrences (ACFE,2020:np). According to Douglas, Burgess, Burgess, and Ressler (2013:20), the culprit during the execution of a mobile fraud is referred to as strategic. These authors also suggest that strategy is a set of learned behaviours that perpetrators created and stick with because they work, but they also accept that it is dynamic and flexible (Douglas *et al.,* 2013:26). They claim that, in any criminal career, regardless of the conditions, the approach evolves with the culprit.

According to Padgett (2015:199), examples information of strategies in mobile fraud investigation may include the following: place, date, and time of the mobile fraud, location of offence, victim's age, number of offenders, amount of planning before a mobile fraud, type of targets, techniques and instruments to be used, methods of committing the mobile fraud, language used, prevalence of precautionary acts, mode of transportation used to and from the mobile fraud scene, and items taken from the victim or mobile fraud scene's.

3.2.2 The techniques used in the commission of mobile fraud

Criminals used different techniques to commit mobile fraud which amongst others include:

Reverse Engineering: Reverse engineering is the process of analysing a technical product to determine how it was built and how it functions (Button *et al.,* 2017:47). A malicious actor can reverse engineer an app to examine the source code and component pieces (Brytting *et al,* 2019:129). The goal is to collect information that can be used to construct malware that exploits an app's functionality or to tamper with an app. For example, an attacker may create their own malicious software to exploit weaknesses uncovered while reverse engineering the banking app (INTERPOL, 2020:np). If the reverse engineering attempt is successful, threat actors will have access to financial data and Personally Identifiable Information (PII) in the app, putting the mobile app publisher and financial institution at risk of revenue loss, fines, and brand reputation damage as a result of fraud (AFCE, 2019:np).

According to SABRIC annual statistical reports-2018/2022, social engineering techniques played a pivotal role in the perpetration of digital banking fraud throughout 2022. Cyber criminals relied on various methods, such as spear phishing, whaling, smishing (SMS phishing), business e-mail compromise, vishing, pretexting and angler phishing (Button *et al.,* 2017:52). SABRIC (2018:np) indicated that these techniques were often employed individually or in combination, forming part of broader fraudulent schemes. Cyber criminals enlisted unsuspecting individuals to serve as intermediaries or 'mules' in their illicit activities. These people are generally attracted by promises of fast money or job possibilities, which are often delivered via online marketing or phishing schemes. Once recruited, the mules are instructed to open bank accounts in their own names. According to SABRIC (2019:np) mobile fraud techniques are widely used in digital banking crimes.

SABRIC also claims that criminals conceal the illicit origins of funds by using complex transactions and movements of funds through multiple accounts or financial institutions to obscure the money trail and make it difficult to trace the source of the money. Fraudsters can reverse engineer an app to examine the source code and component elements.

They can then use that information to create their own harmful app (such as a bogus online banking app) or exploit existing app vulnerabilities (INTERPOL, 2020:np). Man-in-the-Middle (MitM) Attack: A MitM attack occurs when a fraudster intercepts network traffic between a financial institution and its customer. A bad actor, for example, can create a rogue Wi-Fi network that would pass a client's payment data to them once the customer connects to the hotspot (Seleka, 2018:np).

Repackaging: Repackaging is the alteration of a legitimate mobile application by cyber thieves who carefully put malicious code within it before sharing it via unapproved sites. A repackaging attack begins with an attacker reverse engineering a programme, putting malicious code into it, and then republishing the altered app via unapproved marketplaces. According to ISPA (2020:np) as it appears to consumers as if they have downloaded the correct programme, and the software appears to them as authentic (Button *et al.,* 2017:55). However, the counterfeit programme contains code that steals personal information, redirects funds, or engages in other criminal conduct.

Overlay Attacks: An overlay attack is defined as an attacker-generated screen that displays on top of the legal application's user interface (GSMA, 2020:np). To the unaware victim, it would appear to be a normal experience within the app, but they would be entering sensitive information, such as usernames, passwords, credit card numbers, or other personally identifying information, into a form controlled by the attacker. According to AGSA (2019:np) any information entered into the malicious window is delivered directly to the attacker. The victim of this deception is unaware that they have just supplied their personal information. Overlay assaults are used for social engineering as well as data hijacking. They can be used to fool consumers into installing additional malware or doing insecure operations on their mobile devices, such as giving a malicious app complete control over their phones (SABRIC, 2018:np).

Rogue Keyboards: There are various respectable replacement keyboard applications available in the app marketplace that may be used to replace the native keyboards on mobile devices. For example, some of these keyboard programmes may contain vulnerabilities that attackers can exploit, or they may be rogue and created expressly to collect keystrokes and communicate them to an attacker (ACFE, 2021:np). According to SABRIC (2021:np) 93 % of all mobile transactions in 20 countries were flagged as fraudulent in 2019 and a report on the condition of malware, mobile, and fraud produced by a mobile technology company was released. An anti-fraud platform that detects and rejects fraudulent mobile transactions, most of which are caused by ad fraud malware was established which, had protected 31 mobile providers across 20 countries by the end of 2019 (INTERPOL, 2020:np).

Fraudsters appear to target some specific app categories more than others. Ironically, apps designed to improve device functionality and make everyday life easier are the most likely to be hazardous, with 22-32% of malicious apps in 2019 coming into the Tools/Personalisation/Productivity category internationally (SABRIC, 2018:np). Because these categories are particular to the Google Play Store, percentages only apply to apps that have been available on Google Play or still are at the moment. Button *et al.,* 2017:58) indicated that the next most popular categories targeted by hackers are games (18.97%) and entertainment/shopping (15.76 %).

Mobile Banking Trojans: Mobile banking Trojans appear to be legitimate; however, they are simply malware that hide and target a mobile banking app on the device they infect (Button *et al.,* 2017:60). An overlay attack is a typical approach employed by mobile banking Trojans in which a phone screen is placed on top of a legitimate banking application. The malware obtains the victim's authentication credentials and can remain active while further banking activities are carried out (Button *et al.,* 2017:60). For example, malware can alter transaction data by intercepting a money transfer and forwarding it to a false account (Button *et al.,* 2017:62). As smartphone use grows around the world, these attacks are bound to become more common. It is advisable to be cautious when downloading programmes on smartphones and tablets.

Man-in-the-Middle Attacks: In a Man in the Middle attack, the fraudster inserts themselves between the financial institution and the customer, allowing them to intercept, alter, send, and receive communications between the two without raising suspicion. The fraudster hijacks the communication channel between the customer's device and the server by establishing a malicious or rogue Wi-Fi network as a public hotspot (also known as a rogue access point) to facilitate the attack (Button *et al.,* 2017:68). The customer may use a public hotspot without realising they are exchanging payment information across a network controlled by a fraudster. A mobile app's communications should be securely implemented using things like certificate pinning, where the app will only communicate with a certain server. Not doing so makes the app vulnerable to a Man-in-the-Middle attack. Brown (2011:45) argued that fraudsters mentioned that they also use a Man-in-the-Middle attack to inject themselves between a Software Development Kit (SDK) and the destination it is attempting to access. Then they repeatedly hit that endpoint with test calls to determine which ones reflect a successful action. Over time, they determine which parameters are passed to signify a successful installation. They proceed with SDK spoofing once they successfully "install" a programme (Thiel, 2016:67).

SIM Swapping: Swapping a SIM card is a valid service provided by mobile phone carriers when a consumer purchases a new device in South Africa and the previous SIM card no longer works in the new device. A malicious actor can take advantage of this service. According to INTERPOL (2020:np), SIM switching is a malicious tactic in which criminals target mobile carriers to get access to victims' bank accounts, virtual currency accounts, and other sensitive information. A SIM swap involves a fraudster using social engineering techniques to switch the victim's mobile phone number to a new SIM card (Button *et al.,* 2017:73). The fraudster contacts a client's mobile phone carrier and impersonates the customer, persuading a call centre representative to port the customer's phone number to the fraudster's SIM card.

As a result, the user's banking app may be launched on the fraudster's phone (SABRIC, 2021:np). If the bank's authentication mechanism uses text messages to deliver one-time passwords, taking over the victim's phone number becomes an appealing way for a criminal to conduct fraudulent transactions, add payees, or perform other operations during a banking session (Button *et al., 2*017:79).

Although ABSA established using systems to perceive SIM swaps and place holds on banking services, the specific circumstances of mobile fraud cases led to the denial of compensation. Vodacom also contradicts accountability and is defending the matter in court. ABSA declined to compensate a Vodacom client who lost R249,000 due to SIM-swap fraud. The money was taken from a customer’s bank account as the criminals took advantage of online transactions and manipulated the online banking app to commit mobile fraud (Mudiri, 2013:30). Vodacom refused to take accountability. ABSA was unwilling to take accountability as well. In addition to the phishing attempt, the fraudster also swapped SIM cards to capture the randomly created one-time passwords. The method by which someone (in this instance, the fraudster) asks a mobile phone network operator to issue a replacement SIM card for a specific mobile phone number is known as SIM switching (Shulzhenko & Romashkin, 2020:168). indicates that the applicant will often claim that the SIM card was broken or that it was lost. The bank customer's current SIM card will cease to work as soon as a replacement one is given. The new SIM card takes the place of the one that the bank client owns, so all future conversations, including those from the bank, particularly the arbitrarily generated one-time passwords, will be sent to the replacement SIM card (Shulzhenko *et al.,* 2020:169). By swapping an existing SIM card with a newly issued replacement SIM card, the fraudsters are able to intercept the randomly generated once-off passwords required to complete certain sensitive internet banking transactions.

When a victim would call the cell phone provider, the customer would be s instructed to swap the SIM card at a store. ABSA bank takes financial crime very seriously, which is why they launched a thorough forensic investigation into the victim's case. After opting not to pay him back, the matter was brought before the Ombudsman for Banking, who rendered a decision in ABSA's favour. It's crucial to remember that customers also have an obligation to safeguard the Information Technology (IT) devices they use to access their accounts and their own security information, such as passwords and PINs. Service providers (MTN, C-cell And Vodacom) may be victims as well where thieves occasionally exchange their customers' SIM cards without their knowledge (ACFE, 2020:np). Smishing is a type of phishing in which a malevolent actor sends a link to deceive the recipient into clicking on it. When a user clicks on the link, they may be misled into entering their login credentials on a phishing page or unintentionally start the silent download of surveillance spyware on their device. The intention is to obtain illegal access to business, private, and sensitive data that are kept on the device and therefore accessible. The Uniform Resource Locator (URL) is frequently employed in widespread smashing attacks and is also utilised in SMS phishing attempts to lead people to harmful content (AGSA, 2019:np). The hacker deceives the employee of the mobile carrier into installing malicious software, which can be used to get access to the carrier's network and switch the victim's SIM card for the attacker's SIM.

Through digital banking fraud, cybercriminals took about R740 million from gullible consumers in 2022. SABRIC annual crime stats 2018/2022, show a 24% increase in reported cases of digital banking fraud in relation to mobile fraud (SABRIC, 2023:np). In addition, it states that the increasing number of fraud instances involving banking applications and online banking was the main cause of this. In 2022, cybercriminals used digital banking fraud to steal almost R740 million from gullible victims. This is supported by the sources from (SABRIC annual report, 2018/2022) which show a 24% increase in recorded cases of digital banking fraud over the year. It said this was mostly because there are an increasing number of fraud incidents using online and financial applications.

When looking at digital banking fraud across all platforms, SIM-swap incidences climbed by 91% annually, according to the SABRIC (2018/2022). In order to access user accounts and employ one-time passcodes, fraudsters convince the cell provider to do a SIM swap using a fresh SIM card (INTERPOL, 2020:np). As an alternative, thieves can duplicate the victim's SIM card and utilise card copying software to clone it, giving them access to the victim's calls and messages. Thereafter, they can transfer money or make purchases on behalf of the victim (Button *et al.,* 2017:80).

According to Seleka (2018:np), the former minister of water and sanitation, described in his testimony how he was inundated with complaints alleging that individuals on his contact list had been deceived by means of his cell phone number. Cell-C reports that although it has not observed a rise in mobile fraud scams during the shutdown, it is looking into a few of these fraudulent occurrences (INTERPOL, 2020:np). To get private customer information, scammers have been sending fraudulent SMSs to Cell-C subscribers, notifying them that they have won a reward and that they must contact or transfer money. This is a common scam that has been noticed in recent months. Cell-C constantly assesses its security protocols and policies to protect its clients from illicit activity (Seleka, 2018:np). Investigations into some reported mobile fraud cases suggest that the subscriptions are terminated before the charges exceed R200. Most of the time, the lines are deactivated because it seems that they are completely fake. Cell-C protects its consumers from fraud situations by implementing double-opt-in functionality on its network, among other steps.

According to Telkom, unauthorised SIM swaps are the most frequent fraud on their network. In order to ensure that they are dealing with a legitimate customer, Telkom cancels illegal SIM swaps via their call centre. Customers must now go to a store to do a biometric verification. Mobile operators provide consumers with the legal service of SIM swapping, which allows them to exchange their old SIM card with a new one. The SIM cards can be swapped in the following situations:

- A SIM is lost, stolen or damaged;
- A different sized SIM is needed for a new device; and
- The customer is porting out their number onto a different network.

Even though SIM swapping is a helpful and essential service, some people have been motivated to get and utilise the replacement SIM card to access their financial services accounts (SABRIC, 2019:np). Financial companies frequently employ two-factor authentication to give their clients safe and secure services. A popular technique for two-factor authentication is texting the account holder's mobile number with a one-time password (GSMA, 2020:np). The fraudster will have access to calls, authentication messages, and one-time passwords from the victim's financial service provider if the SIM switch has been successfully completed. This enables the transfer of money from the victim's bank and mobile money accounts to the fraudster. Even while SIM switch fraud is a worldwide issue, it is most seen in underdeveloped nations (INTERPOL, 2020:np). In addition to investing in SABI trainings to lower the risk of fraud, service providers are making capital investments to monitor their fraud controls are in accordance with the perceived threats in their markets (Button *et al.,* 2017:83).

As the sector develops and partnership dynamics become more intricate, the potential consequences of SIM switch fraud could increase. One of the most popular techniques for obtaining a customer's personal information, such as account numbers, PINs, and other identifying information, is smishing, sometimes referred to as SMS phishing. Through SMS messages, phishing scammers gain access to the target's mobile phone and steal his/her personal information when the user clicks on a text link in the message (ISPA, 2022:np). The statement by SABRIC (2021:np) indicates that smishing scams are also carried out using mass SMS campaigns, frequently through foreign SMS gateways, in which vast populations of mobile users are targeted with texts that appear to be sent by reputable businesses, such as the mobile provider.

The information is used for various illegal purposes, including:

- Requesting money transfers from the client's mobile money account to a con artist under false pretences (like a prize);
- Using a sim swap to obtain access to a customer's mobile money account and other financial services accounts in order to access their funds;
- Obtaining access to the victim's accounts on social media and other platforms; and selling the victim's private data to third parties.

Smishing communications are made to appear authentic, and they frequently mimic the organisation's style, including the usage of its logo and branding. The victim is taken to a phone website that imitates the actual one but has a slightly different address once they click on the link in the SMS (ACFE, 2020:np). The Nigerian 419 Scam serves as a typical illustration of a smishing scam. Typically, victims receive texts offering incentives to coerce them into sending money or divulging personal information (Brody, Kern & Ogunade, 2022:210). For example, the con artist may pose as someone in dire need of medical attention and requests that the victim sends money to his/her mobile money account so that he/she can receive life-saving medical care. In other situations, con artists may attempt to steal money from the victims by posing as fee and charge collectors while claiming that they must send higher amounts of money abroad. To make these transactions easier, fraudsters would also ask for the victim's bank account information, which they would then use fraudulently (Jansen & Leukfeldt, 2015:28). Several weeks may pass before victims realise, they have been duped and the money they had sent from their mobile money account is gone, depending on the severity of the fraud.

In these circumstances, the client can attempt to hold the mobile money provider accountable for the money lost. But there is more to the liability issue than meets the eye. Whether or not the provider is held financially responsible will depend on several factors, including whether the victim was careless in sending money or disclosing personal information (Jansen & Leukfeldt, 2015:29). However, this puts providers at risk of damage to their reputation, which could erode customer confidence. Therefore, regardless of responsibility, handling these frauds continues to be in the best interest of providers (Button *et al.,* 2017:29).

Mobile banking malware: According to the Nokia analysis, the prevalence of mobile banking on smartphones has led to an increase in banking malware threats. Banking Trojans use screen overlays for bank logins, keystroke capture, and screen captures to obtain user information (Brytting *et al., 2019*:109). Preventive measures are crucial for safeguarding a company because, once activated, a banking Trojan stays in the background, gathering the necessary data for fraudsters. Educating customers about cybersecurity will be a major component of these measures. Although emails may contain links to download a bogus programme that can steal personal information, phishing is still a very real concern. The goal of both vishing and smishing is the same (Button *et al.,* 2017:51). Scammers can use phone calls and direct SMS messages with spoof caller identification to look like they are from reputable banks or online retailers, tempting victims to download and install malicious programmes. Fake apps that were discovered on Google Play and the Apple App Store often received over 100,000 downloads before being removed. There is a great chance that account takeover scammers will be successful (SABRIC:2021:np).

In this scheme, the con artist deceives their targets into voluntarily sending them sizeable bank transfers. The attempt to deceive supply partners, publishers, or advertisers by taking use of mobile advertising technologies is known as identity fraud and attribution fraud (Wells, 2015:77). Fraudsters aim to steal from advertising budgets when they use this strategy. There are several variations of identity fraud and attribution fraud, including click spam, phone installs, and phone impressions (INTERPOL, 2020:np). For instance, dishonest publishers looking to profit from erroneous impressions may purposefully position an advertisement out of view or jam it into a single pixel to generate views or impressions that never happened (SABRIC, 2018:np).

Device cloning: As costumers use online retailers, bank accounts, and other practical banking apps, the quantity of personal information saved on mobile devices is growing. In order to make calls and make purchases without having to examine their smartphone, fraudsters copy the original device and transfer all its data to it. The owner is then billed for these transactions (Button *et al.,* 2017:31). Unidentified hackers cloned the state security minister and her deputy's cell phones in South Africa. According to an official, calling the incident 'concerning.' Cloning a device involves imitating the identification code of a real mobile phone to get access to the network. In this case, unauthorised phones that use real identification codes are used. Mobile phone chips are used to copy and embed data from one phone into another (Lokanan, 2015:54). This kind of fraud causes the phone unit to be used repeatedly, with users possibly unaware that they are using a clone. Fraudsters utilise a scanner to gather the identification codes from public locations. There are several places to do this activity, including as airport terminals or parked cars near major roads with scanners installed. Since the identification codes on digital mobile phones are encrypted, no such fraud has been found to date.

***Subscription fraud*:** Refers to joining a mobile phone network using fake identity information. Often, this kind of fraud goes unnoticed until a bill is unpaid. It is also possible to clone the aforementioned mobile phone, which would allow many instances of the phone to use the same account.

Phishing: Criminals trick customers into giving them private or sensitive information by using deceit. Vishing and phishing remain the most popular techniques (SABRIC annual statistical reports-2018/2022). Despite this, digital banking has become more popular (Chandra & Calderon (2005:103). However, criminals have modified their social engineering strategies to take advantage of data from social media and data dumps, making their attempts to deceive clients harder to detect. The most common fraud techniques in the field of digital banking fraud persist to be social engineering techniques, which include, but are not limited to phishing, fishing, smishing, email hacking and business email compromise (Thiel, 2016:55). These techniques are frequently combined or applied as a single part of a larger plan. Phishing uses emails to send a target to a "spoofed" website that appears authentic, tricking victims into entering their login credentials. According to Prabhakar (2014:43), vishing which has become much more common in 2020, involves thieves calling prospective victims and posing as bank representatives in order to coerce them into divulging personal information. Once the criminals have access to the victim's account, vishing may be used as a follow-up tactic to trick the victim into giving them the verification token such as an OTP that is needed to finish a transaction (Thiel, 2016:57).

The login credentials for banking applications were frequently compromised due to "vulnerabilities" in the way that such data were managed. For instance, the credentials can have been stored on the device in another location. Prabhakar, Ross and Jain, (2004:66). The login and password might have been used for several different apps for a significant increase in banking app fraud was caused by cell phone snatching (AGSA, 2021:np). The author did clarify that this does not mean that the problems lie with the applications. According to SABRIC (2021:np) there were no complaints of the banking app software being compromised to carry out the fraud. The right credentials are needed to access the app, even though there are several methods and strategies involved in the cell phone snatching mode of operation. These credentials may have previously been compromised through social engineering techniques like shoulder surfing or phishing.

Phone theft: describes a scenario in which an unauthorised user uses a lawful phone that has been lost or stolen. It is also possible to clone a stolen cell phone. There are variations in the number of fraudulent uses of phone networks depending on the area. For example, it is anticipated that 30% of all calls made in SABRIC as a whole are fraudulent (SABRIC, 2021:np). In the banking sector, mobile fraud is pervasive and poses a higher danger to government businesses. According to Marohn (2016:33), mobile fraud is still the main and enduring threat that SABRIC faces. Information technology, forensics, psychology, accounting, auditing, and management are all involved in fraud studies (Lokanan, 2015:76). These days, anti-fraud specialists frequently employ the fraud triangle to elucidate the circumstances that may encourage people or businesses to commit fraud. The model can also be used to draw attention to general industry or economic factors that may raise overall risk. Professionals in anti-fraud search for the following three elements to determine risk: Opportunity, justification, and motivation (SABRIC, 2021:np).

Identity theft: occurs when someone steals personal information that can be used to identify them. This may occur, for example, when technology is used to examine or retrieve an individual's identifying details, possibly in conjunction with a rogue agent or a mobile money provider employee (SABRIC:2021:np). In addition, malware activity, smishing/SMS scams, data breaches, and insecure mobile internet browsing can all lead to identity theft. Lokanan (2015:76) contends that smishing/SMS fraud is the most popular technique for obtaining identification information by going straight after end users in nations where feature phones predominate in mobile devices. Identity theft is still a significant issue globally, even with significant investments made in information security measures. For instance, in 2014, over two-thirds of South Africa households' names, addresses, phone numbers, and email addresses were made public due to a data security breach at the country's biggest bank.

Over a ten-year period, the number of identity theft cases reported at SABRIC climbed by 125%, reaching 175,000 in 2018/2022. More recently, 11.5 million consumers' personal information was compromised by a major mobile operator due to a data breach. These occurrences imply that, although putting money into data privacy safeguards is crucial, doing so is insufficient to combat the risks of identity theft and data breaches (Lokanan, 2015:89).

3.3 LEGISLATIVE FRAMEWORK OF MOBILE FRAUD

The legislative frameworks that regulate the SABRIC are discussed in this section. Based on the country's internal realities, international obligations, and constitutional models, South Africa has developed strong anti-fraud and ethical models, including extensive and reliable policy papers and legislative tools (SABRIC, 2018:np). These criteria are furthered by a variety of domestic laws, plans, strategies, and regulations, which also provide guidance to various stakeholders on how to create and carry out suitable measures to prevent and deal with corrupt activities. Wilhelm (2014:101) asserts that in order to combat the issue of fraud and corruption occurrences, the nation needs anti-fraud laws and policy guidelines. It should be highlighted, therefore, that while the following legal principles apply for the purposes of this section, the investigation of fraudulent activity is not limited to the law (Wells, 2015:112). The common law and several specialised laws, some of which are included below, both control South Africa's legal frameworks pertaining to fraud:

3.3.1 Financial Intelligence Centre Act (No. 38 of 2001)

The Financial Intelligence Centre Act, 2001 (Act 38 of 2001), empowers the FIC to apply measures designed to identify the proceeds of crime, combat money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction. The Financial Intelligence Centre Amendment Act of 2017 (No. 1 of 2017) was endorsed to strengthen South Africa's ability to combat financial crimes, including money laundering, terrorist financing, and other illicit activities. The Amendment Act expands the goals and functions of the Centre and clarifies the application of the Act in respect to other laws.

This Act also defines or clarifies key terms and expressions and in addition, renames the SABRIC subject matters experts as the Financial Fraud Advisory Council (FFAC):

- The more clarified certain provisions;
- The updated reference to legislation;

- To provide the sharing of information by the centre and supervisory bodies; to provide for the issuance of directives by the centre and supervisory bodies;
- To establish an appeal board to hear appeals against decisions made by the centre or supervisory bodies and to make further provisions for offenses;
- To provide for matters connected therewith.

The FFAC also allows for the registration of accountable and reporting institutions to clarify the roles and responsibilities of supervisory bodies. It also provides written arrangements relating to the respective roles and responsibilities of the centre and supervisory bodies, authorises the centre, supervisory bodies to conduct inspections by the centre and supervisory bodies. The establishes an appeal board to hear appeals against decisions made by the centre or supervisory bodies. To makes further provisions for offences and provides for matters connected therewith. It also allows for the registration of accountable, reporting institutions to clarify the roles and responsibilities of supervisory bodies. It also provides written arrangements relating to the respective roles and responsibilities of the centre and supervisory bodies.

In accordance with Section 2 of the FICA (No. 38 of 2001), the FICA was founded to safeguard South Africa's financial system, grow its economy, and act as a responsible member of the international community. FICA (No. 38 of 2001) was created with the intention of establishing and maintaining an efficient regulatory framework, compliance models, and operational capability to detect and prevent crime, mobile fraud, and the funding of terrorism. The FICA (No. 38 of 2001) gathers, processes, and evaluates information disclosed or acquired under the Act to monitor, advise responsible institutions, supervisory bodies, and other individuals.

The National Anti-Corruption Advisory Council was founded to provide recommendations to the Minister of Finance regarding optimal protocols and strategies for identifying illicit activity proceeds and thwarting mobile fraud. The National Anti-Corruption Advisory Council also serves as a venue for parties to interact with one another and provides advice to the FICA (No. 38 of 2001) regarding execution of its duties. The National Anti-Corruption Advisory Council, corruption is one of the greatest impediments to the country's growth and development, and the rebuilding effort begun three years ago must be maintained. The Council consists of representatives from various government agencies, accountable institutions and supervisory bodies which must be consulted before the Minister of Finances can establish or modify any aspect. The repeal FICA (No. 8 of 2001) regulations, alter the list of accountable institutions, supervisory bodies, or reporting institutions, or exempt anyone from FICA (No. 38 of 2001) compliance. Identification and Verification: The FICA (No. 38 of 2001) stipulates that those responsible institutions should know their business partners for the mobile fraud control measures to be effective. The Act mandates that each person

or entity with which a transaction is concluded must be identified and verified before any commercial ties can be formed or transactions can be completed.

Identification and verification are provided to both new and current clients in accordance with established protocols based on four categories: partnerships, trusts, legal people, and natural persons. Furthermore, members are excluded from compliance in some situations.

Records: The prevalence of the business relationship or transaction, the persons involved, and all character identification and verification documents and/or copies obtained prior to establishing a commercial partnership must all be documented by accountable institutions. If clients acquire new products or make changes to already-existing products, client information must be updated. Records must be preserved for a minimum of five years beyond the day the transaction is completed, or the relationship is ended, whether they are stored physically or digitally. If there is easy and free access to the records, the responsible institution may designate a third party to maintain records on their behalf. In the event that the designated record storage is not met, the responsible institution is still accountable. The only way that authorised centre representatives can access records to examine, extract from, or copy any such records is through a warrant that has been issued in chambers by a magistrate, regional magistrate, judge, or other official of the jurisdiction in which the records, or any portion of them, are kept. A portion of these records may be used as evidence in court.

Reporting: All responsible institutions are required by the FICA (No. 38 of 2001) to report financial transactions that meet a certain threshold or frequency of occurrence. There are a number of long-term insurance exceptions that are free from reporting requirements. These include life and medical policies; investments in unit trusts or on stock exchanges; and provident funds, pension funds, and retirement annuities. Accountable institutions also have a duty to notify the Centre of any transactions that seem odd or suspicious. These include operations that have no discernible commercial or legal purpose and are carried out in order to get around the FICA (No. 38 of 2001) requirements, such as receiving, transferring, or laundering money, the proceeds of illegal activity, or property linked to funding terrorist activities and associated activities. The Commissioner for SARS stated that accountable institutions are required to create and execute internal policies for identity verification and identification, as well as record management and storage systems, techniques for identifying transactions that need to be reported, and other prescribed matters. To guarantee adherence to the FICA's requirements, responsible institutions must also designate a compliance officer and train their staff, as noncompliance is a crime for which there could be punishment.

3.3.2 Public Finance Management Act (No. 1 of 1999)

Accounting officers are held responsible for the resources they utilise even as the Public Finance Management Act (No. 1 of 1999) gives them the management tools they need. It creates broad best practice models and distinct lines of accountability that managers can use or modify as needed. Setting treasury norms and standards for local government and providing for related matters are the goals of ensuring sustainable. The sound management of the financial affairs of municipalities and other local entities. Guarantees, indemnities, and the supply of security by specific state organs are governed under Section 66 of the PFMA (No. 1 of 1999), along with any other transaction that binds or may bind [the public entity] to any future financial commitment. According to Section 75 of the Municipal Finance Management Act [MFMA] (No. 56 of 2003), municipalities must post important papers and data, such as the Integrated Development Plan (IDP) annual report, annual budget adjustments, and documents and policies connected to the budget, on their website.

The Local Government: Municipal Finance Management Act (No. 56 of 2003) intends:

- To secure sound and sustainable management of the financial affairs of municipalities and other institutions in the local sphere of government;
- To establish treasury norms and standards for the local sphere of government; and
- To provide for matters connected therewith.

3.3.3 Prevention and combating of Corrupt Activities Act (No. 12 of 2014)

The main legislation governing anti-bribery and corruption enforcement in South Africa is the PCCAA (No. 12 of 2014). It covers both domestically based businesses and foreign-based businesses that conduct business in the nation. People in positions of power are required by Section 34 of PCCAA (No. 12 of 2014) to report certain violations over R100,000. Opinions on whether the obligation to report relates solely to crimes committed by persons inside the pertinent domain of a person's authority or to any specific offence vary. A small number of people benefit financially from corruption while the great majority suffer. Corruption hinders economic growth and keeps people from taking advantage of economic opportunities (Wilhelm, 2014:66). Additionally, it implies that businesses may miss out on profitable transactions in the public sector, for instance, if one of the businesses gains an unfair edge over the other businesses through

bribery or other forms of corruption. An example would be that the governing bodies of all organisations are required to manage risks, prevent corruption, and adhere to all relevant laws, rules, codes, and standards.

Numerous recent local and international situations have served as further evidence for this. PCCAA (No. 12 of 2014) among other pieces of legislation, and South Africa's frequency on the Organisation for Economic Cooperation and Development (OECD) mandate that proactive measures be taken to prevent and combat bribery and corruption. Therefore, the need to implement an anti-bribery and corruption compliance programme cannot be evaded/ shirked by organisations.

3.3.4 Banks Act (No. 94 of 1990)

The Banks Act (No. 94 of 1990) was enacted with the following goals in mind to regulate and oversee the operations of publicly traded organisations that accept deposits from the general public, as well as to address related problems. Banking rules are, in general, the legal guidelines that apply to the Bank and the operations it occasionally conducts. Together, the FICA (No. 38 of 2001) and PCCAA (No. 12 of 2014) rules are referred to as the Banking Rules. Banking Rules can refer to either the FICA (No. 38 of 2001) and PCCAA (No. 12 of 2014) rules. Protecting the public by policing and overseeing the organisations that accept deposits is one of the main goals of the BA (No. 94 of 1990), the Banks Act, the SARB Act of 1989, and the South African Reserve Bank Act of 1989. Section 5 of the Banking Act defines 'banking business' as accepting deposits (except from partial payment for specific goods or services) and making advances of funds, along with other financial operations specified by regulations issued under the BA (No. 94 of 1990). The Section 54(3) of BA (No. 94 of 1990) governs the transfer of rights, obligations, and assets that come with combining banks, as well as the transfer of a bank's assets and liabilities to another bank or to an individual the Registrar of Banks has allowed. Apart from the aforementioned, South Africa is a signatory to multiple international legislative frameworks and engages in worldwide campaigns and forums that impact the battle against fraudulent activities, both directly and indirectly.

SABRIC preventing organised crime, sharing legal aid, recovering assets, combating mobile fraud, beneficial ownership, open government, and transparency. International endeavours additionally foster corporate ethics, which aids in the battle against fraud within national borders. Additionally, there are regional instruments that address certain fraud-related issues, such mobile fraud. The models distinguish between theoretical, qualitative, internal, and external industrial aspects while taking into account a number of requirements and possible regions of effect on fraud practice (Button *et al.,* 2017:80). The elements from outside the banking industry that have an impact on fraud management are

represented by the external factors, whilst the internal factors are bank-specific and interbank issues. The models start with the essential element of the fraud: the individual or perpetrator and their motivation (Button *et al.,* 2017:100).

Therefore, the pressure, opportunity, and rationalisation components of Cressey's fraud triangle serve as a representation of the first component of the models (Cressey, 1953:47). The second element consists of internal industry factors, which include things like information sharing, interbank competitiveness, organisational traits, insider involvement, internal controls, and information technology that can both encourage and discourage fraud. The external industry elements make up the third component (Wells, 2015:34). These encompass legal elements such as legislation, regulation, and law enforcement, in addition to the overall governance framework. At this point, the broad use of information technology in society is also taken into account (Wilhelm, 2014:89). In addition, political, economic, and customer aspects are taken into account. The third component comprises theoretical and qualitative variables, such as lack of centralised database, unemployment, severity, certainty, and celerity (Sarah, 2012:28).

3.3.5 Fraud Act 2006

The principal anti-fraud law at SABRIC, the FA (2006), unlike the earlier laws it replaced, created a precise legal definition of fraud for the first time at SABRIC. It also eliminated the requirement of deception as a component of this type of criminal activity for the primary offences it established (INTERPOL, 2020:np). Sections 2, 3, and 4 are the major three newly constituted crimes apart of several others. The Fraud Act 2006 also establishes new offences for dishonestly procuring services and for manufacturing, possessing, and distributing items intended for fraudulent purposes.

- If someone violates any of two sections, which outline various ways to commit the offence, they are guilty of fraud.
- The sections are as follows: (2) fraud by false representation; (3) fraud by withholding information; and (4) fraud by abusing one's position.
- A person who is guilty of fraud is liable - (a) on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum (or to both); (b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both).

A representation could be made explicitly or subtly. Section 2: False Representation Fraud, the act of deceiving someone through fraud is illegal. There must be dishonesty in the depiction. The representation

must be made with the goal to profit or to put another person at danger of losing something. It is not necessary for the profit or loss to truly occur. If someone makes a deceptive representation knowing it is, or could be, false or misleading, then it is considered false (Button *et al.,* 2017:44). Any representation regarding a truth or legal matter, including one on an individual's mental state, is considered a representation. It can be expressed verbally or through actions. The manner in which the representation must be expressed is not restricted. It might be expressed verbally, in writing, or online. Behaviour can also imply a representation (Button *et al.,* 2017:47). A case of representation by conduct would be someone who deceitfully utilises a credit card for purchases.

A person would be fraudulently claiming to have the permission to use the card for that transaction by submitting it (Button *et al.,* 2017:58). Whether or not the business receiving the card for payment is duped by the representation is irrelevant. This offence can also be committed by someone who participates in “phishing” which refers to the practice of falsely disseminating an email to a large audience under the pretence that it is from a reputable financial institution (Wells, 2015:56).

The email asks the recipient for personal information, including bank account and credit card data, so the "phisher" can obtain the financial details of other people. If a representation or anything suggesting one is delivered, in any format, to a system or apparatus intended to receive, transmit, or process communications (with or without human assistance), it may be considered created (Button *et al.,* 2017:37). This provision's primary goal is to guarantee that fraud can be perpetrated in situations in which a person represents him/herself digital technology like online phone banking and an automated answer is generated without the requirement for human intervention. When there is a legal need to disclose information to another person, omitting to do so constitutes fraud. Legal obligations to divulge information can arise from both written and verbal contracts (Button *et al.,* 2017:108). This clause would encompass, for instance, a solicitor's failure to disclose valuable information to a client during their working relationship to deceive the client. This sentence is incomplete; it does not make sense. The dishonest abuse of one's position to commit fraud is illegal under Section 4. It is applicable in cases in which the defendant has been granted privileges and is therefore required to protect the financial interests of others or refrain from acting in a way that might jeopardise those interests (ACFE, 2020:np).

Since the term "abuse" is meant to encompass a broad spectrum of behaviour, it is not defined. Both positive action and omission can result in the commission of the offence. Many cybercriminals employ social engineering to extract personal information from gullible users in order to carry out fraudulent transactions, since mobile cell phones and specialised apps become an appealing target for fraudsters (SABRIC:2021:np; Marakalala, 2023:25). In many situations, mobile applications, spam, and weak

passwords have all contributed to the loss of financial and personal data, providing criminals with a profitable opportunity to target and steal victims' identities. Social engineering techniques are employed by criminals because they find it easier to take advantage of people's innate tendency to trust others.

3.4 SUMMARY

This chapter details the levels of mobile fraud and also presented the prevalence of mobile fraud in the South African banking business, as well as how to prevent mobile fraud, specifically in the South African banking sector. This is followed by an overview of mobile fraud at SABRIC. Furthermore, the chapter discusses the extent of mobile fraud at SABRIC,

the prevalence of mobile fraud in the SABRIC and legislative framework of mobile fraud at SABRIC that has evolved over time. It is vital that the most recent and accurate information be obtained from the most credible sources. Given the fact that the majority of banks now utilise their customers' mobile phones as an additional means (second factor) to identify and authorise credit, a user's mobile identification has become a prime target for fraudsters. Based on the many methods and models for recognising financial crime in mobile fraud, this growing problem calls for a thorough strategy to uncover hidden risks in mobile fraud. combating financial crime is challenging since many internal control systems have serious weaknesses. The most crucial aspect of technology is its ability to maintain comprehensive records of all completed tasks and electronic transactions involving fraudulent activity or higher fraud risk.

CHAPTER FOUR

FACTORS CONTRIBUTING TO MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

4.1 INTRODUCTION

Incidents of financial fraud dent the reputation of the SABI to its customers while causing financial losses to all stakeholders. This chapter discusses factors that contribute to mobile fraud in South Africa. The emerging use of these technologies has not only benefited societies but also attracted fraudsters and criminals to abuse technology for financial benefits. The factors discussed in this chapter include corruption, unemployment and poverty, as well as climate change and substance abuse.

4.2 FACTORS CONTRIBUTING TO MOBILE FRAUD IN THE SABI

4.2.1 Corruption

Corruption is a major problem that has negative and devastating effects to victims. In developing countries, the adverse consequences of corruption include murder as well as impoverishment of victims (SABRIC:2020:np). When personnel partake in corruption that involves embezzlement of funds, they require a place to conceal the funds. Although most nations have laws and regulations requiring banks to do various checks to identify the proceeds of corruption, most banking institutions rarely abide by such restrictions. As a result, they enable fraudulent activities involving money laundering. The United Nations (2018:np) claims that Banks and Dirty Money reveal the warped incentives at the core of this problem. This organisation recommends that among mitigating factors, holding senior executives accountable for bank rule violations is the best course of action, as failing to do so would perpetuate banks' support for corruption and the damage it causes (SABRIC:2021:np). AGSA (2020:np) argues that the largest obstacle preventing markets in nations, especially those in Africa, from realising their full potential in spite of having important resources, is corruption. The South African government can design an Identity Book (ID) that is deemed unforgeable and incorruptible, but the crucial element remains the employees of the department in charge of issuing it at large, as fraud is invariably the result of corruption and bribery (ACFE, 2018:np).

In South Africa, it is not uncommon to read (both in print and online media reports) about public officials possessing numerous identity documents and/or passports, or about citizens opening bank accounts or defrauding reputable companies out of millions of rand using identification of annual statistical reports-2018-2022 (SABRIC:2021:np). Therefore, the country should assess whether the tools it has to combat fraud are effective. It can be argued that the country needs technologies that can be used to combat the causes of corruption as well as those of social engineering (ACFE, 2018:np). For example, Experian, a company that reports on consumer credit once announced that it had suffered a data breach that may have given a suspected fraudster access to personal information of about 24 million South Africans and 793,749 businesses (SABRIC:2021:np).

South Africa struggles to combat unacceptably prominent levels of corruption. The culture of corruption is so pervasive in South Africa that it affects both public and private sectors. SABRIC (2022:np) states that in particular, most corruption manifests in the form of nepotism, state capture, poor management, irregular procurement, fraud, bribery, as well as extortion. Deeds of corruption enable corruptors to self-enrich themselves unlawfully. Indicators of the negative effects of corruption in South Africa include the deteriorating economy, subpar service delivery, and an extremely dissatisfied citizenry (The United Nations, 2018:np). One likely enabler of corruption is moral decay and unethical decision-making processes especially at the highest levels (SABRIC, 2020:np).

Although corruption is not exclusive to South Africa, the way the nation handles corrupt practices or corrupt actors is deplorable. For example, despite reports and in some cases, evidence of corrupt deeds, South Africa seems to lack decisive measures to enforce accountability and suitable repercussions. The scourge of corruption in South Africa is deeply ingrained and if not addressed, can be institutionalised and normalised. SABRIC (2022:np) lists consequences of corruption in South Africa includes Politically Exposed Persons (PEPs) and examines the procurement and tendering procedures for Personal Protective Equipment (PPE) during the COVID-19 era. Such corrupt deeds were committed by officials who had the power to influence procurement or tender procedures (ACFE, 2020:np). The report by the SABRIC (2022:np) also reveals ambiguities and governance failures and warns that the public procurement tender system is vulnerable to misuse. Normally, corrupt deeds are performed by people who have political connections or officials employed in the public or private sector.

Money launderers target to escapes in the financial system used to transfer money (SABRIC, 2022:np). The rampant incidences of corruption in South Africa requires solutions to address. The following are the four main goals shown in the report:

- To raise awareness of high-end financial flows and signs of grand corruption involving PEPs among financial institutions, law enforcement, and prosecuting authorities;
- To create networks for law enforcement, financial institutions, and other organisations that deal with high-end corruption practices to exchange information about risk, trends, and typologies;
- To help financial institutions develop typologies and indicators related to money laundering and financial flows that may be linked to corruption; and
- To further assist law enforcement and criminal prosecutions by identifying the patterns and flows associated with corruption.

The corruption that has plagued South Africa has hindered developments in needy communities, jeopardised democracy, damaged the reputation of the nation, and deterred foreign investment, all caused by lack of faith in the nation's capacity to combat corruption effectively. ACFE (2018:np) shows that among the most common corrupt practices in South Africa is the acquisition of government procurement budgets. In fact, such corruption leads to diversion of procurement budgets meant to uplift communities and improve the economy (SABRIC, 2020:np). The misuse of funds meant to mitigate the negative impacts of the COVID-19 pandemic exposed South Africa's degree of self-enrichment. All of these elements point to the necessity for effective measures that can counteract corruption and lessen its negative effects on society (Button *et al.,* 2017:54).

Another form of financial fraud is theft of information on companies, including company names, contact information, bank account information, and VAT numbers. It is probable that these confidential details are accessed illegally and sold to unauthorised buyers, even if there is not any concrete proof of how it got online. A research study conducted in 2018 revealed that it cost R14, 000 to purchase a complete set of someone's personal information from the dark web (Coppolino *et al.,* 2015b). While files lost by Experian during the hack were recovered, the success of the hacking activity exposed a vulnerability of the nation to cyberattacks and the dire need to address the underlying issue of the low uptake of digital identities, particularly in the business sector (ACFE, 2018:np). Following the report on the aforementioned breach, SABRIC collaborated with Experian and identified clients that could have been affected by the breach and measures were taken to safeguard their personal data henceforth (SABRIC, 2016:np).

It is important to note that, the organisation pointed out that the arrest of high-ranking perpetrators may have contributed to a 39% decline in bank robbery instances involving clients who deposit cash (United States Agency for International Development, 2017:np). In fact, there were 9% fewer recorded cases of mobile banking fraud in 2022. Furthermore, the percentage of occurrences using SIM swaps decreased from 87% in 2021 to 76% in 2022, suggesting that the effectiveness of this fraudulent strategy is decreasing (Coppolino *et al.,* 2015b).

4.2.2 Unemployment and Poverty in the South African Society

In its annual report on crime statistics in 2022, SABRIC (2022:np) detailed financial fraud and security breaches. The statistics included details on contact crimes, digital offences, application fraud, and card fraud (Open Data Charter, 2018:np). The impact of crime on South Africa's economic prospects is significant as shown in a report by the World Bank which aimed to contribute to a better understanding of the impact of crime on South Africa's economic growth. Additionally, the high rate of incidences of violent crimes occurring on a regular basis in South Africa renders crime a serious issue (SABRIC, 2022:np). It is of the utmost importance to address this scourge since the country is consistently ranked among the top five in the world for homicide rates. Theft of crucial infrastructure networks is another form of organised crime that is increasing in South Africa. The mobile fraud on that collapse crucial projects meant to develop communities is an economy that shows increasing unemployment. Since the global financial crisis of 2008–2009, the real gross domestic product (GDP) has been declining, and since 2015, GDP per capita has been shrinking on average (ACFE, 2021:np). The socioeconomic consequences have been poor, characterised by widespread unemployment, poverty, and inequality (ACFE, 2021:np). As a result, the country experiences extremely high levels of poverty and unemployment. Under such conditions, it is crucial to address specifically financial crime, particularly that which hamper socioeconomic growth (SABRIC, 2022:np).

The government has resolved to make combating crime a top policy priority. This research highlights the necessity of adopting several approaches. Although addressing crime is complicated and necessitates long-term solutions, past experiences in South Africa and elsewhere indicate that targeted, well-designed, and executed policies can be prioritised for effective short- and medium-term crime reduction. Regulatory reforms, law enforcement actions, and targeted violence prevention programmes are examples of such policies and practices (ACFE, 2021:np).

These align with the government's present priorities. The report further emphasises that sustainably decreasing crime necessitates tackling the underlying causes associated with socioeconomic issues such as unemployment and poverty.

In poor countries, corruption enabled by puny measures to address financial crimes has deadly consequences and traps many people in poverty (SABRIC:2020:np). Financial crime is a term used to refer to all crimes committed by an individual or a group of individuals that involve taking money or other property that belongs to someone else, to obtain a financial or professional gain (SABRIC, 2019:np).

4.2.3 Climate Change Relating Crime of Mobile Fraud

While the phenomenon of climate change has been widely used in agriculture, it is also used in the banking sector. Climate change has had an effect on the banking industry, including mobile fraud in banking sectors by causing outages and vulnerabilities, disrupting infrastructure, and possibly raising the risk of cyberattacks. The high and unpredictable frequency of occurrence of hurricanes and other extreme weather events have damaged communication networks, including those that financial institutions use for online banking. There rarely exists a clear-cut connection between mobile fraud and climate change, but as digital banking and mobile money systems become more popular, fraudsters may be able to take advantage of weaker populations and financial systems due to the possibility of climate-related disasters and resource shortages (INTERPOL, 2020:np). A rise in the use of digital banking changes the climate, but as digital banking becomes more popular, fraud risk rises as well (Marakalala, 2023:24). The increasing sophistication of fraudsters' methods is one of the main causes of the rise in fraud by means of digital banking, making it more and more difficult for banks and their clients to identify and stop fraudulent activities (SABRIC, 2021:np; Open Data Charter, 2018:np). It is imperative to grasp and understand these variables for financial establishments and banks to adopt pre-emptive actions to secure the assets and data of their clientele, as well as for individuals to defend themselves from monetary damages and identity theft (SABRIC, 2022:np).

The frequency of digital banking fraud has increased because of the sophistication of fraudsters' techniques used to take advantage of loopholes in online and mobile banking systems (Annalise, 2022:21). Nevertheless, there are hazards associated with this ease of use, including viruses that can steal login credentials, phishing attempts, and account takeover (ACFE,2021:np). Mobile banking is so convenient and user-friendly, and therefore it has grown in popularity. Nevertheless, compared to desktop computers, mobile devices are also more susceptible to financial crime and cyberattacks.

Users should also be informed about the best ways to secure their mobile devices. While ATMs make cash availability convenient, they are also susceptible to fraud, such as hacking and skimming (Annalise, 2022:21). Via skimming transactions or installing malicious software, thieves can obtain credit card information from ATMs. The ATM fraud can have serious repercussions, such as bank account cancellations and monetary losses. The ATM fraud, security measures like upkeep, transaction monitoring. Be specific are main causes of high level of crime, including mobile fraud (Marakalala, 2023:26). Digital Payment Systems are becoming easier to access and more convenient thanks to digital payment platforms like PayPal. They do, however, also offer fresh opportunities for scammers to take advantage of mobile transfer by kidnapping high profile businessmen (SABRIC, 2022:np).

Non-standardised procedures such as inadequate compliance monitoring decrease compliance checks due to interbank rivalry and SABI (AGSA:2021:np). The reasons behind fraudsters' success include: a culture where fraud is tolerated; high transaction costs that lead to system abuse; inadequate compensation that encourages cash-handling staff to steal; a lack of training and frequent communication; seasonality fraud is more common during holidays; certainty; celebrity; severity; pressure; unemployment; and the absence of a centralised database for fraudsters (SABRIC:2021:np). A model comprising three main elements namely pressure, opportunity availability, and rationalisation of the behaviour or attitude may account for the rise in fraud (Wells, 2015:67). Factors contributing to mobile fraud include non-standardised processes (failure to abide to MF), poor compliance monitoring, interbank competition leading to reduced compliance checks, information sharing, hence, reduced confidentiality, organisation culture (some societies are generally lenient to fraudsters) (SABRIC:2021:np). Normally, high cost of transactions may lead to system abuse such as poor remuneration of employees, theft of cash, weak pricing policy, maturity of the mobile fraud services, poor awareness (lack of training and frequent communication), seasonality-fraud is high during festivity, certainty, celebrity, severity, pressure, unemployment, and lack of centralised database for fraudsters (Brytting, *et al.,* 2019:88).

The Annual Crime Statistics Report for 2022 published by SABRIC reveals a concerning increase in financial crime that has resulted in the loss of almost R3.3 billion. These crimes, which include digital fraud, card fraud, and contact crimes, undermine economic growth in South Africa. According to Zinn and Dintwe (2015:55), the South African Police Service (SAPS) uses independent police officers to accompany suspects to document locations they indicate; a practice aimed at ensuring objectivity and reliability in investigations. Systems may become exposed as a result, making them more appealing to scammers. According to INTERPOL (2020:np) a more thorough breakdown may be found:

- **Increased Reliance on Digital Systems**

Climate-related disasters: Floods, droughts, and wildfires are examples of natural disasters that can disrupt the traditional banking system and increase reliance on mobile money services and banking.

Acceptance of mobile money: Vulnerable groups may find mobile money services even more crucial as a result of financial hardship and displacement brought on by climate change, making them targets of mobile fraud.

- **Vulnerabilities in Digital Systems**

Fraudulent schemes: The emergence of climate-related crises can serve as a catalyst for criminal activity, including schemes that target disaster relief funds or capitalise on the increasing usage of mobile banking.

Exploitation of vulnerabilities: Scammers may target individuals experiencing financial difficulties as a result of climate change in order to steal their money or data using tactics like phishing or identity theft techniques.

- **Environmental Crimes and Financial Crime**

Money laundering: Two instances of environmental crimes that can generate significant amounts of money that call for money laundering are illegal logging and wildlife trafficking. The use of mobile money systems could simplify this process.

Fraud involving disasters: Criminals may use mobile money to conduct fraudulent schemes involving disasters linked to climate change, such as construction fraud or insurance fraud.

- **Examples of Climate Change and Crime Interconnection**

Reduced Availability: Criminal organisations may have more opportunities to exploit weaker groups and perpetrate crimes if there is less food or water available due to climate change.

Organised Crime Networks: As a result of climate change, organised crime groups may exploit weaknesses such as destitution or displacement to expand their activities and perpetrate new crimes.

Fraudulent Green Investments: The use of mobile money to facilitate fraudulent green investment schemes allows criminals to target individuals or groups interested in funding climate solutions.

- **Infrastructure Disruption**

Communication System Damage: Natural disasters like hurricanes brought on by climate change have the potential to destroy vital infrastructure, such as telephone lines and the internet, which are necessary for mobile and online banking.

Outages and Service Disruptions: Fraudsters may be able to take advantage of vulnerabilities when there are brief or extended disruptions in banking services due to disrupted infrastructure.

- **Increased Vulnerabilities**

Reduced Security Measures: To preserve some degree of service during times of infrastructure disruption, banks may need to temporarily reduce security measures, which leaves them more vulnerable to cyberattacks.

Vulnerability Exploitation: Cybercriminals can initiate fraudulent activities, such as account takeover fraud or unauthorised transactions, by taking advantage of system disruptions and compromised security measures.

- **Cyberattacks**

Complex Cybercrimes: Criminals are increasingly employing cutting-edge technologies, such as AI and machine learning, to carry out complex attacks that are challenging to identify.

Growth in Dependency on Digital Channels: People are more susceptible to cyberattacks as they depend more and more on digital channels, such as mobile apps, for banking.

Social Engineering: Social engineering techniques are used by scammers to fool users into disclosing personal information, which can result in fraudulent transactions or account takeovers. Phishing and vishing are strategies that use phone emails or phone calls to fool users into divulging personal information.

- **Mitigation Strategies**

Robust Cybersecurity Measures: To defend their systems and data against cyberattacks, banks should make significant investments in cybersecurity measures. Enhanced Authentication: By implementing multi-factor authentication, accounts can be protected from unwanted access.

Fraud Detection and Prevention: Fraudulent transactions can be found and stopped with the use of sophisticated fraud detection and prevention systems.

Customer Education: Customers can lower their risk of becoming victims of fraud by learning about common fraud schemes and self-defense techniques.

Cooperation: To fight cybercrime and safeguard the financial system, banks, governments, and other stakeholders should work together.

4.2.4 Substance Abuse

There is a close relationship between drug abuse and crime. Drug abusers commit crimes to pay for their drugs, and this inflicts damages to the society (Rafaiee, Olyaee & Sargolzaiee, 2013:55). Moreover, most criminals commit crime while under the influence of drugs. It may be for this reason that some criminals commit mobile fraud to fund their lifestyle. Several studies have linked crime with substance abuse variables in the past. The individual factors like drugs or mental illnesses could explain about 40 % of crime variance (cases of crime). The direction of this suggested association between these variables is unclear and drug use could act as a risk factor. The crime related to substance abuse including most of commercial crime like fraud, corruption and money laundering which involved mobile fraud to scam the SABI costumers.

4.3 SUMMARY

Among factors that contribute to mobile fraud in South Africa, as discussed in this chapter, are digital fraud, card fraud, as well as contact crimes. These, among others, undermine economic growth in South Africa. Corruption is a major problem which has a devastating human cost. In poor countries, it kills people and traps millions more in poverty. Also described in the chapter is the definition of the term financial crime, which refers to all crimes committed by an individual or a group of individuals that involves taking money, other property that belongs to someone else, to obtain a financial and professional gain. The likely effect that the frequent and unpredictable events associated with climate change have on digital banking was also discussed.

CHAPTER FIVE

CHALLENGES ENCOUNTERED BY FORENSIC INVESTIGATORS IN INVESTIGATING MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

5.1 INTRODUCTION

Mobile phones have various operating systems, new technology, and software applications. Even though mobile phones are small enough to fit in a pocket, improvements in computational power and semiconductor technology have increased mobile phone efficiency. As a result, it is challenging for forensic investigators to review evidence using a mobile device. Mobile fraud may not be easy to detect and therefore needs thorough investigation and therefore this chapter provides a discussion on the challenges encountered by forensic investigators in the investigation of mobile fraud at SABRIC. Furthermore, the discussion will also include the future of mobile fraud in the SABRIC.

5.2 THE CHALLENGES ENCOUNTERED BY THE FORENSIC INVESTIGATORS IN THE INVESTIGATION OF MOBILE FRAUD IN THE SABI

Data from mobile devices are frequently utilised effectively and form a crucial component of forensic investigations. It is crucial to have a complete understanding of forensic tools and their properties to extract relevant data (Marakalala, 2023:np). This study examines the prevalence of some of the newest forms of information that may be used as mobile phone evidence. Also, it discusses a number of more recent technologies and how well they work to gather evidence from phones (SABRIC, 2019:np). A review of the limitations and potential applications of mobile forensic technology, as well as mobile device features and mobile forensic investigation procedures, is also included in this thesis. Mobile fraud represents a subdivision of digital forensics concentrating on the extraction and evaluation of information from mobile devices (Davis & Pesch, 2013:472). This information may consist of call logs, text messages, emails, photos, videos, browsing history, and application data. ACFE (2021:np) indicates that mobile fraud can be employed to investigate various offences, such as homicide, theft, fraud, and child exploitation. Additionally, it can be utilised to identify cyber threats, including malware and data breaches (PwC, 2022:np). To lessen cybercrime, the South African government has launched efforts, including the creation of SABRIC whose duties include supplying the nation's banking institutions with pertinent information about risk management and crime (Marakalala, 2023:28).

Most people use their phones daily, and a large number of them fall prey to various illegal activities (Annalise, 2022:21). The possibility of using smartphones for illicit purposes has grown along with the market's continuous growth. The challenges associated with obstacles hindering investigations on mobile fraud is encryption, various platforms, cloud storage, device locks, App security, rapid technological advancements, legal issues, fragmented data, tampering detection, and data overwriting (SABRIC, 2020:np). Mobile device forensics involves the extraction and examination of digital evidence from smartphones, tablets, and other portable devices. It serves as an essential tool for probing cybercrimes including fraud, identity theft, phishing, malware, and espionage (PwC, 2022:np). Nevertheless, mobile device forensic investigators encounter numerous obstacles that complicate their work. Below are some of the primary impediments (SABRIC, 2021:np):

- ***Device variety***

There is a wide variety of mobile devices on the market, each with its own operating system and file system. This can make it difficult to develop and use forensic tools that are compatible with all devices. With numerous embedded applications, operating systems, and hardware parts, mobile devices are intricate systems. According to Davis and Pesch (2013:477), examining mobile fraud necessitates a thorough comprehension of these technologies as well as the capacity to analyses data saved in various formats.

- ***Encryption***

Many mobile devices are encrypted, which can make it difficult to access and analyse data. Since mobile devices frequently use encryption, it might be challenging to access data without the right encryption keys or passwords. Forensic investigators find it difficult to recover data from these devices because of this (Annalise, 2022:20).

- ***Data volatility***

Data on mobile devices can be easily overwritten or deleted. This can make it difficult to recover evidence. Mobile device data can readily be wiped by fraudsters intentionally or by routine use. This may result in the loss of important information, which would complicate the investigation (Casey, 2021:32).

- ***Legal considerations***

Several legal factors need to be acknowledged when carrying out mobile fraud investigations (SABRIC, 2020:np). These factors involve obtaining a warrant, preserving evidence, and adhering to privacy laws.

- ***Diversity of devices***

Mobile devices are available in a multitude of shapes, sizes, models, and operating systems. Each device might possess distinct hardware specifications, storage capabilities, encryption techniques, security features, and data formats (Button *et al.,* 2017:69). This implies that forensic investigators must have access to a broad array of tools, techniques, and protocols to manage various devices. They also need to stay informed about the ongoing updates and developments in the mobile device market and technology (PwC, 2022:np).

- ***Remote access***

Since mobile fraud can be perpetrated remotely from any location in the world, it might be difficult to find and follow the offender. Moreover, fraudsters can conceal their identity and location by using virtual private networks and other anonymising technologies (SABRIC, 2021:np).

- ***Lack of standardisation***

Data storage and transfer protocols are not standardised between various mobile device manufacturers, operating systems, and applications. Because of this, forensic investigators may find it difficult to obtain and examine data from various mobile device kinds (Marakalala, 2023:29).

- ***Differential levels of technological expertise***

People with different levels of technological expertise utilise mobile devices. This implies that while some users might unintentionally change or remove important data, others might try to conceal or remove data in order to thwart an inquiry (PwC, 2022:np).

5.3 THE FUTURE OF MOBILE FRAUD

Mobile fraud associated with the use of mobile devices is a sophistication that is rapidly advancing, and the security industry is introducing innovative tools and methodologies to address it. SABRIC (2020:np) reports that mobile fraud serves as an essential resource for law enforcement, cybersecurity, and civil lawsuits, and will likely become more significant in future (INTERPOL, 2020:np).

These should be tools that can be used to tackle mobile fraud are that designed specifically to retrieve data from mobile devices, namely, forensic tools (Casey, 2021:21). Two methods have been employed to deal with this situation: either shortening the period of time between the phone's release and the availability of mobile device forensic software for that phone or setting a benchmark to assess a tool's utility on a particular device (PwC, 2022:np). One of the biggest forensic issues with the mobile platform is the possibility of information being accessed, stored, and synchronised across several devices (PwC, 2022:np). It takes more effort to keep the data secure because it is fragile and easily altered or removed from a distance (Casey, 2021:38). In contrast to computer forensics, mobile fraud presents forensic investigators with fresh challenges. PwC (2014:np) indicates that digital evidence from mobile devices is typically difficult to gather for law enforcement and forensic investigators. Some of the causes are as follows:

Hardware Disparities: Numerous mobile phone models from various manufacturers are available in the market. Forensic investigators may encounter a range of mobile phones, contingent upon the device's dimensions, configuration, hardware, capabilities, and operating system (PwC, 2022:np). Moreover, new models are frequently released because of the quick product development cycle. As the mobile environment expands, examiners must be able to adjust to new obstacles and stay up to date on mobile device forensic procedures (Bair, 2017:55).

Network Careers Differ: Finding the phone is the initial step in any mobile phone inquiry. It is impossible for even experienced investigators to identify a phone just by looking at it because of the various network providers (PwC, 2022:np). It is possible for a hardware vendor to sell a portion of its functionalities under multiple carrier names. To safeguard user information, privacy and security measures are in place on contemporary mobile platforms.

These traits serve as a roadblock during forensic gathering and evaluation. Andrea, Olivier, Yann, Serge, and Gianluca (2014:10) states that encryption techniques are integrated into modern mobile

devices from the hardware to the software levels. In order to obtain data from the devices, the examiner might have to circumvent several encryption methods (Annalise, 2022:20).

Data Preservation: It is critical to stop the affected smartphone from accepting any further voice or data calls during an inquiry. Since SMS messages are kept in a "First In, First Out" fashion, newer messages may overwrite older ones. Incoming calls have the ability to erase call history logs in full, and if a device is not secured against incoming communications, it can be remotely cleaned of all data.

Consequently, mobile phones need to be stored in a wireless storage container when they are originally purchased (PwC, 2022:np). There are various strategies that can be applied, with differing levels of effectiveness.

Inadequate Resources: As said earlier, the quantity of forensic examination tools needed will rise in tandem with the number of mobile devices (PwC, 2022:np). To obtain such devices, forensic acquisition equipment such as power cords, chargers, and adapters for different cell phones must be kept on hand (Afonin & Katalov, 2021:12). Digital media investigations are made more challenging by anti-forensic techniques such as data hiding, obfuscation, falsification, and secure deletion.

Power and Connectors: Keeping their phones charged is another issue that investigators face. Afonin and Katalov (2021:16) state that a phone's battery will ultimately run out if it is left unplugged for an extended amount of time. Because many mobile devices store data in RAM, a complete loss of power could result in the loss of data and, consequently, important evidence (PwC, 2022:np).

Data Formats: Like the other components of a modern mobile phone, most of the information that an investigator seeks to located in a fixed location or format. Data files might be kept in many places. As previously noted, specific SIM cards have the ability to save data in the phone's memory (Annalise, 2022:20). RAM is divided into two types: non-volatile RAM, which is found in mobile phone hardware, and volatile RAM, which needs an electrical charge to maintain its contents (which maintains data without an electrical charge). It is important for investigators and developers of forensic software to be aware that information can be found in any of these memory types.

Inconsistency of Evidence: Digital evidence can be easily corrupted, whether on purpose or accidentally, (Barker, 2018:79). For example, browsing an app on a phone may change the data associated with that app.

Changing the Operating System of a Mobile Device: It is possible to move programme data, rename files, change the device's operating system, as well as changing the manufacturer's operating system. The suspect's expertise and experience should be taken into account in this case (PASA, 2016:np).

Availability of Tools: There is a multitude of different smartphones available. According to PASA (2016:np), it is necessary to use a range of tools because one tool might not be able to support every device or carry out every necessary task. Choosing the right tool for a certain phone might be challenging.

Legal Issues: Criminals conduct cross-border crimes via mobile devices. To address these pertinent law enforcement concerns, the forensic examiner needs to be informed on both the severity of the offence and the applicable local laws (PASA, 2016:np). The combination of different systems and devices and the live network connection are complicating matters. Power shortages are one problem that could cause security mechanisms to reactivate. The remote destruction of important data is another issue (PASA, 2016:np). Time limits and the lack of experience provide challenges for investigators trying to examine a smart phone or device on a network system. However, there is no standardised procedure in place for investigators to gather information from these devices to support their inquiries (OECD, 2023:np).

The sheer quantity of networks and device manufacturers: Even if the specifics of each device's inspection may vary, the examiner may ensure that the data gathered from each smartphone is sufficiently recorded and that the results are repeatable and defendable in court by using the same examination techniques (OECD, 2023:np).

Banking App kidnappings are on the rise in South Africa: A concerning new criminal trend has been observed in South Africa: victims are being abducted and forced to transfer money from their banking apps, frequently under threat of violence (Ambe, 2024:35). This results in the victims losing all of their savings or entirely looting their other accounts.

5.4 SUMMARY

This chapter summarised the literature study on challenges encountered by the forensic investigators in the investigation of mobile fraud at SABRIC. Such investigations have scale economies and network effects, need a significant amount of capital, and are governed by regulations for prudential purposes. Building a customer base and making a profit takes time because of consumer switching costs. Organisations are impacted by fraud in a number of ways, including psychological, operational, and financial. The total impact of fraud on a business can astounds, even while the financial loss resulting from it is considerable. The harm to one's good name, relationships with customers, and goodwill can be severe.

CHAPTER SIX

BEST PRACTICES BY DEVELOPING A CONCEPTUAL MODEL TO COMBAT MOBILE FRAUD IN THE SOUTH AFRICAN BANKING INDUSTRY

6.1 INTRODUCTION

The chapter presents practices that are considered the best in combating mobile fraud by SABRIC. Among best practices are the use of various techniques in the detection of mobile fraud. Furthermore, forensic investigation framework models are sketched in support of the best practices as benchmarked from different sources. This chapter will deeply focus on the best practices by developing conceptual model to combat mobile fraud at SABRIC.

6.2 THE BEST PRACTICES IN COMBATING MOBILE FRAUD

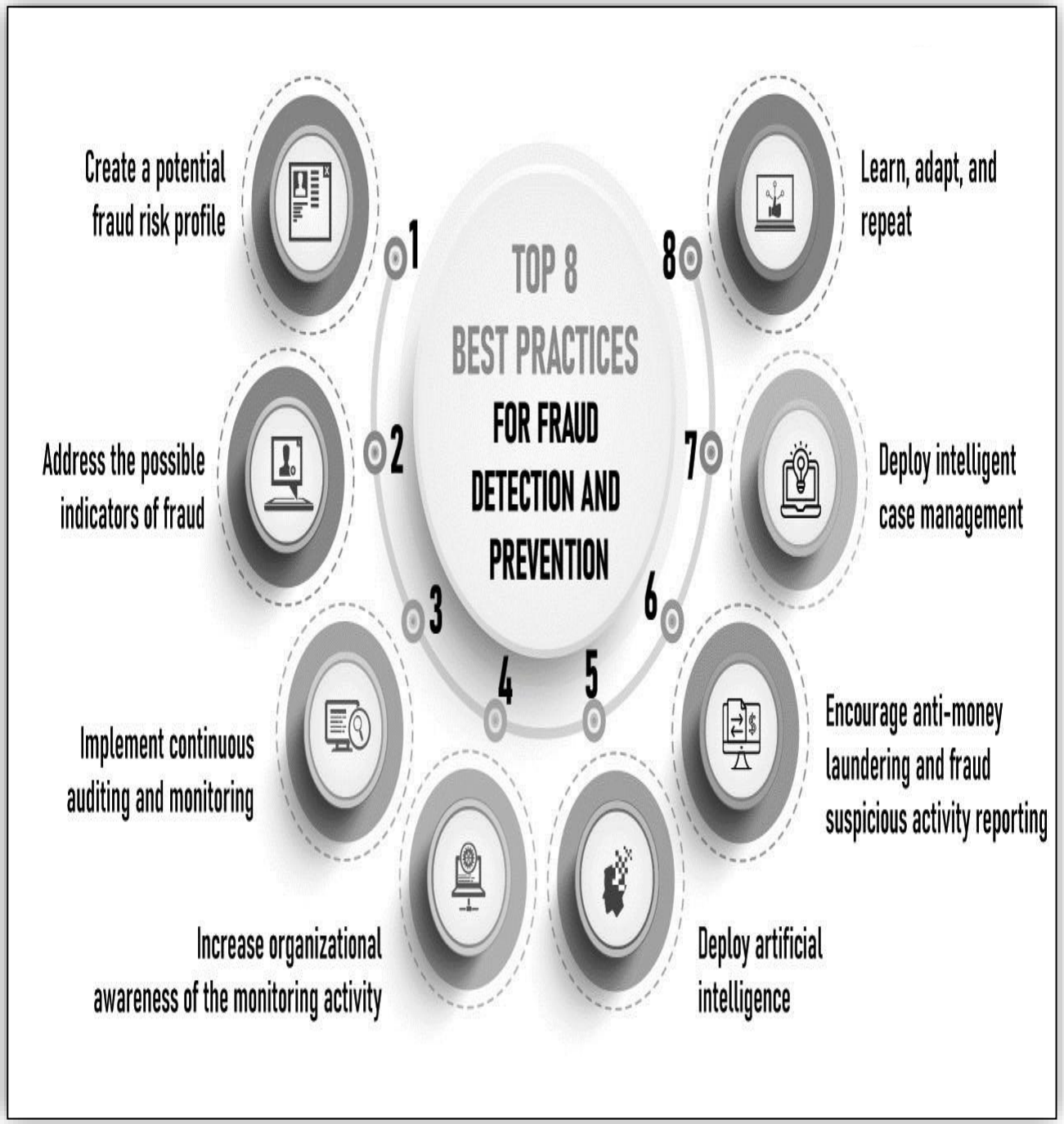
Mobile fraud remains a major concern at SABRIC and in any sector that involves the management of finances. Although ripe with positive innovation in the SABI (Nedbank, FNB, ABSA, STD and Capitec) channels and solutions also mean new avenues for fraudulent activities to take place and new vulnerabilities that can be exposed (Button *et al.,* 2017:18). Players across the ecosystem need to work together and continually improve security measures to keep bad actors at bay and protect the funds and data of the end users they serve (INTERPOL, 2020:np). Below is the presentation of best practices that may be applied in the prevention of mobile fraud:

Continuous monitoring and adaptive strategies: Proactive actions and continuous observation are necessary for the continuous process of fraud prevention. Companies should invest in sophisticated fraud prevention tools, regularly train staff on fraud detection techniques, conduct thorough audits to identify risks and vulnerabilities, and review and update their fraud prevention strategies to stay ahead of evolving threats (AGSA, 2019:np).

Education for end users: When providing goods and/or services directly to customers, it is critical to make sure they are equipped with the most recent information necessary to use products securely. By providing end users with fraud education, they may protect their financial resources by making wise judgments and taking the necessary precautions (Brytting *et al.,* 2019:101). Customers are less likely to become victims of fraud unintentionally if they are aware of prevalence scams or risks related to certain fintech goods. From the bottom up, user-initiated alerting systems can be helpful in highlighting any unauthorised or questionable activity occurring on a financial platform (AGSA, 2022:np).

Provide an easily accessible route, like a dedicated fraud reporting hotline or email address, for customers to report fraudulent activities. Encourage users to report any suspicious or unlawful transactions as soon as possible (Button *et al.,* 2017:22).

Figure 6.1: Top 8 Best Practices to Combat Mobile Fraud



Source: (Button *et al.,* 2017:106)

The above-mentioned figure presents mobile fraud detection challenges faced by subject matter expects and underneath are discussions based on the figure.

***Create a potential mobile fraud risk profile*:** This pertains to a top-down approach to risk assessment, which outlines the business units and types of mobile fraud that could happen in the locations where mobile fraud is most likely to happen (ACFE, 2022:np).

Next, as part of the overall risk assessment, it is necessary to categorise the risks based on the organisation's entire risk exposure and create risk profiles for mobile fraud that involve all stakeholders and decision-makers.

***Address the possible indicators of mobile fraud*:** While sampling might be helpful for identifying issues that are generally consistent across datasets, this is not always the case when mobile fraud is involved. Instead, organisations should evaluate all of their data. Mobile fraud transactions are by their very prevalence premeditated (ACFE, 2022:np). It is said that transactions may not be reported even when they fit under the parameters of some regular tests.

***Implement continuous auditing and monitoring*:** Continuous auditing and monitoring can be used to assess and validate the efficacy of an organisation's controls over transaction authorisations. Continuous analysis could involve writing scripts to identify anomalies as they appear over time (PwC, 2022:np). The total effectiveness, consistency, and quality of SABRIC in the mobile fraud process can all be significantly enhanced by this procedure.

***Increase organisational awareness of the monitoring activity*:** One crucial component of combating mobile fraud within the firm is the programme internal communication, which serves as a valuable tool for doing so (PwC, 2022:np). If employees are aware of the preventative measures that have been implemented, they would not engage in mobile fraud, which can be a very successful preventive strategy (Button *et al.,* 2017:93).

Encourage mobile fraud suspicious activity reporting: Finding clients implicated in financial crime or mobile fraud is the goal of the investigation that follows Suspicious Activity Reporting (SAR) (Omar & Bakar, 2012:15). A specific behaviour could be included in SAR if it gives rise to suspicions that the account holder is trying to hide anything or carry out an illegal transaction. As a result, businesses must put policies in place to report financial irregularities connected to mobile fraud (Button *et al.,* 2017:63).

Deploy intelligent case management: According to the AGSA (2022:np), utilise an advanced, analytics-driven, intelligent case management solution that can automatically assist in the following ways:

- Set case priorities, suggest investigative measures, and expedite simple cases;
- Add information to alerts regarding related accounts, beneficiaries, or customers;
- locate and retrieve data with intelligence from a third-party data source or from an internal database;
- Display information in comprehensible graphic aids;
- SAR should automatically fill out and be ready for electronic filing, if required.

The SABRIC can streamline their mobile fraud investigations by deploying an intelligent case management solution to aid their fight against cybercrimes (KPMG, 2013:19).

Learn, adapt and repeat: Reviewing, reassessing, and restructuring one's mobile fraud profile is necessary in order to move investigative lenses in line with the most prevalent of mobile fraud schemes as well as those that are mainly related to the risks that are particular to organisation (INTERPOL, 2020:np). This can be accomplished by monitoring controls that application control settings cannot control and by utilising data analytics to identify ineffective or non-functioning control areas (Omar & Bakar, 2012:66). Lastly, patterns and mobile fraud indicators shown by mobile fraud detection tests and continuous monitoring and auditing processes need to be investigated.

Mobile fraud reporting policy and procedure: Managers must be aware of what to do in the event of a scam or any alarming sign of mobile fraud so that they can act quickly (Patidar & Sharma, 2021: 2233). According to the National Treasury (2020:34), the goal of the mobile fraud reporting policy and procedure is to ensure that action may be performed quickly and effectively:

- To prevent losses of funds or other assets and to maximise recovery of losses where mobile fraud has occurred;
- To minimise the occurrence of mobile fraud by taking rapid action at the first signs of a problem;
- To identify the mobile fraudsters and maximise the success of any disciplinary or legal action taken;
- To minimise any adverse publicity for the organisation suffered as a result of mobile fraud;
- To identify any lessons learnt and use these to prevent mobile fraud in the future and to reduce adverse impacts on the business of the organisation.

The statement by the ACFE (2020:np) report acknowledges the existence of a mobile fraud reporting policy and procedure which may, in itself, help to act as a deterrent, as it shows that an organisation or a company is prepared to defend itself against the risk of mobile fraud:

- To reduce the possibility of identity theft and allow businesses to confirm the identity of their clients. Through the collection of pertinent data and comprehensive identity verification procedures, businesses may create a solid base for preventing fraud;

- Encryption, Multi-Factor Authentication (MFA) and frequent security audits are examples of data security techniques that can help protect sensitive data from unauthorised access;

- ***The application of AI and Machine Learning (ML):*** This has the potential to improve fraud detection performance to a great extent. These technologies are capable of real-time analysis of enormous volumes of data in order to spot trends and abnormalities that could point to or highlight fraudulent activity;

- This incomplete to replicate identifier, biometric authentication which uses fingerprint or facial recognition which can increase user account security and lower the danger of unauthorised access;

- ***Transaction monitoring:*** Real-time transaction monitoring systems that examine consumer behaviour and transaction trends are helpful to identify hazards or possible fraud before it spreads (Button *et al.,* 2017:109). Creating guidelines and standards to identify suspicious activity, such as transactions that are abnormally big, occur frequently in a short period of time, or originate from high-risk areas, is an essential part of a solid security foundation;

- ***Two-Factor Authentication (2FA):*** Requesting an extra authentication factor from clients, such as a special number sent to their mobile device, can aid in confirming their identity while logging in or conducting high-risk transactions;

- ***Device recognition:*** It can be used to recognise and verify client devices that are used to access accounts or start transactions. This assists in identifying and thwarting attempts at fraud from unidentified or hacked devices.

Using behavioural analytics, one can analyse and find anomalies in consumer contact patterns. By establishing baseline behaviours for each customer, unusual activities, such as sudden changes in transaction types or deviations from established patterns, can be flagged for investigation. Pattern recognition: these algorithms can help identify similarities and correlations among fraudulent activities across different customer accounts. Identifying patterns can detect fraud rings or organised fraud attempts.

6.3 THE USE OF FRAUD DETECTION TECHNIQUES

One of the best practices is the usage of fraud detection techniques. Fraud detection techniques are divided into two broad spectrums. Each one has its sub-techniques:

6.3.1 Statistical Data Analysis Techniques

Statistical data analysis for fraud detection completes several statistical tasks, including fraud data collection, fraud detection, and fraud validation, by carrying out in-depth investigations. The following sorts of techniques are subdivided from these:

Statistical parameter calculation: The process of computing various statistical parameters, including averages, quantiles, performance indicators, and probability distributions, for fraud-related data gathered during the data collection process is known as statistical parameter calculation (Salkind, 2014:43).

Regression analysis*:* To examine the association between two or more variables, regression analysis is utilised (Salkind, 2014:45). An estimate is also made of the relationship between the independent and dependent variables. This facilitates the comprehension and recognition of connections among many fraud attributes, in addition to forecasting potentially fraudulent activities in the future (Salkind, 2014:51).

Probability distributions and models: This method is used to map models and probability distributions of different types of fraudulent business operations, either in terms of discrete parameters or probability distributions (Salkind, 2014:53).

Data matching: When comparing two sets of acquired data about fraud, data matching is employed. Algorithms or programmed loops can be used to carry out the procedure. Additionally, for marketing, security, and other purposes, data matching is used to eliminate duplicate entries and identify connections between two datasets (Salkind, 2014:62).

6.3.2 Artificial Intelligence

Companies have improved their internal security and streamlined corporate processes by deploying artificial intelligence for fraud prevention (ISPA, 2020:np). AI has emerged as a critical tool for preventing fraud at financial institutions due to its increased efficiency (ACFE, 2020:np). AI based fraud techniques include the following methods:

Data mining: Data mining for fraud detection and prevention automatically classifies, clusters and segments data and finds relationships and rules in the data that may indicate intriguing patterns, including fraud trends (Salkind, 2014:78).

Neural networks: Neural networks under fraud detection perform classification, clustering, generalisation and forecasting of fraud related to data that can be compared against conclusions that are raised in internal audits or formal financial documents (Patidar *et al., 2*021:39).

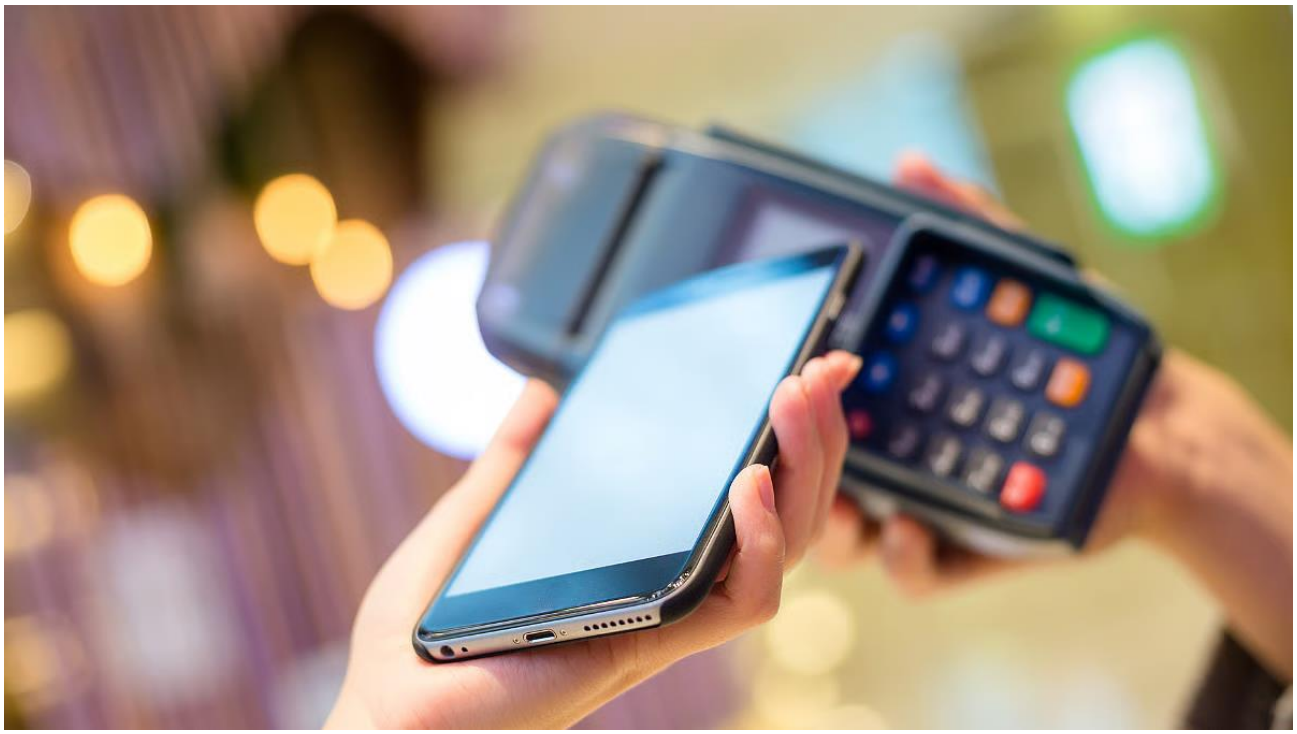
Machine learning: The possibility of detecting fraud using machine learning is made possible by its ability to learn from past fraud trends and identify them in subsequent transactions (McKinsey Global Institute, 2015:10). Machine learning makes use of both supervised and unsupervised learning techniques. In supervised learning, a random subset of every data is manually categorised as 'fraudulent' or 'non-fraudulent' (McKinsey Global Institute, 2015:16). Conversely, unsupervised learning makes predictions without additional labelling by looking for common patterns (fraud, for example) and correlations in the raw data (INTERPOL, 2020:np).

Pattern recognition: Pattern recognition algorithms detect approximate classes, clusters or patterns of suspicious behaviour, either unsupervised or supervised. Other techniques such as link analysis, Bayesian networks, decision theory and sequence matching are also used for fraud detection (ACFE,2020:np).

Express kidnapping when disclosing banking details leads to financial loss: The banks have increased security on their online platforms, making it more difficult for criminals to acquire costumers' financial information, as criminals of kidnappings by commonly coercing victims into divulging their online banking passwords (Ndlovu, 2023:np). According to ISPA (2020:np), all available money from the victim's accounts including accessible house loan accounts and credit balances is moved to mule accounts in the middle or withdrawn, using different ATMs. It is concerning that significant levels of violence have been reported in a number of documented incidents. Moreover, SABRIC (2022:np) puts forth that it is important to remember that although the strategy is commonly documented in express kidnapping cases, comparable tactics are also used in some kidnapping-for-ransom scenarios.

In some cases, the attackers use ATMs to take available cash out of the victim's accounts while also threatening to demand a ransom from the victim's relatives. The statement by SABRIC (2022:np) that criminals are now migrating to banking app shakedowns and other methods since the previously popular Sim-swap method is proving to be less effective than in the past.

Figure 6.2: Banking App Kidnappings Profiling



Source: Ndlovu (2023:np)

The implications of mobile banking are being felt across South Africa's financial environment as a result of a frightening increase in daily kidnappings (Ndlovu, 2023:np). As digital transactions become more prevalent, experts warn that the very security measures intended to protect users may actually increase the length of hostage situations (SABRIC, 2022:np). The necessity for increased vigilance is highlighted by the way criminals are changing their tactics to take advantage of these shifting payment methods. A concerning new trend in crime has surfaced in South Africa: victims are being abducted and forced to transfer money from their banking apps, frequently under fear of violence. This results in the victims losing all their savings or their other accounts being fully looted (Ndlovu, 2023:np). A growing number of incidents involve the kidnapping or hijacking of people to force them into giving up unlawful access to their banking applications (Ndlovu, 2023:np). A variety of identification techniques relates to particular aspects such as the victim, the offenders, the points of compromise, and fraudulent expenditures.

Online purchases are made using the victims' accounts both domestically and internationally. There are various techniques utilised to execute these extortions. It is virtually impossible for law enforcement to trace the funds when victims are compelled to deposit money into bank accounts situated outside of the country. In some cases, online payments are conducted using the victims' accounts, both within the country and across borders (Ndlovu, 2023:np).

In another scenario, members of the criminal organisation keep the victim confined while making multiple digital wallet payments or account transfers to a nearby location, all the while moving around and quickly extracting cash from ATMs (Button *et al.,* 2017:137). Standard banking application security measures, including biometric identification, facial recognition, and pin codes, fail in every case (PwC, 2022:np). There is not much that can be done in an app kidnapping in which the victim is instructed to access their own profile on their own device (Zinn & Dintwe, 2015:49). It is similar to when someone uses their own card and pin to force the victim to take withdraw from an ATM at gunpoint (Ndlovu, 2023:np).

Customers are advised to educate themselves on the strategies employed by criminals and make sure that the required steps are taken to prevent abduction because prevention is key to this kind of crime (PwC, 2022:np). While increased awareness may help prevent certain occurrences, it is not a panacea. The Head of Nedbank's digital channels and subject matter specialist suggests the following course of action for victims of banking app shakedown in the worst-case scenario:

- ***Cooperate:*** The lives of the victims or clients should always come first. It is best to comply if someone is threatening to use violence against clients or victims.
- ***Stay calm:*** Strive to maintain composure. It is critical to maintain composure because panic might make things worse.
- ***Memorise details:*** If the victims or clients are able, mentally record any distinguishing characteristics, appearance, or accents of the attackers. Law enforcement may find use for this material in the future**.**
- ***Stay passive:*** Steer clear of any abrupt or hostile movements that can agitate the abductors.
- ***The victim must comply with syndicate demands****:* The target should comply with syndicate instructions, such as accessing banking apps. The victim's personal safety should always come first.
- ***Seek help later:*** Once the situation is resolved, the victim should contact the authorities and bank immediately to report the incident.

SABRIC (2019:np) also keeps tabs on criminal activities linked to banking and furnishes data on the many kinds of banking offences. According to its Annual Crime Stats 2018/2022 report, while banking app fraud cases increased by 36%, other types of mobile banking crimes showed a decline (ACFE, 2020:np). This suggests that as the once-popular Sim-swap method is proving to be less frequent and effective than in the past, as criminals are using other methods such as banking app shakedowns. Positively, there was a 9% decrease in the quantity of mobile banking fraud instances that were recorded in 2022 (Button *et al.,* 2017:117):

***Regulatory Models*:** The laws, regulations, and standards that control IPS's administration, monitoring, and oversight as well as the roles and obligations of its stakeholders comprise the regulatory models for fraud prevention in IPS (INTERPOL, 2020:np). The models' goals are to safeguard users and guarantee the IPS's security, dependability, and integrity. In order to combat fraud in IPS, the models also direct and promote technology advancements as well as user education initiatives (ISPA, 2020:np). Compared to developing countries, developed countries have models that are more detailed and standardised. For instance, in the European Union (EU), a uniform legal foundation for fraud prevention in IPS across member states is provided by the Payment Services Directive (PSD2) and the Regulatory Technical Standards (RTS). Strong Customer Authentication (SCA) and Common and Secure Communication (CSC) are requirements set forth by the PSD2 and the RTS for payment service providers to implement for electronic payments. These measures improve IPS security, innovation, competitiveness, and confidence (AGSA, 2021:np).

As a result of a number of issues, including a lack of funding, regulatory experience or coordination, institutional or legal hurdles, and a lack of resources, developing nations have fewer established or fragmented models (ACFE, 2018:np). For instance, there may be several regulators in several African nations overseeing various kinds of payment service providers, leading to discrepancies or holes in the IPS's fraud prevention regulations (OECD, 2023:np). Furthermore, regulations specifically for IPS or fraud prevention in IPS, some developing nations rely on generic laws or regulations for consumer protection or electronic payments.

Technological Solutions: Technologies including biometric authentication, blockchain, AI, machine learning, encryption, tokenization, and cloud computing are examples of solutions for IPS fraud prevention. By authenticating users, analysing transactions, confirming data, safeguarding information, and facilitating transaction traceability and audibility, these solutions can improve the security and effectiveness of IPS (AGSA, 2021:np).

User Awareness: A crucial component of IPS fraud prevention is user awareness, which entails giving users the knowledge and tools they need to defend against scammers and report questionable activity. Enhancing user awareness can be accomplished in a number of ways, including encouraging users to report any anomalies or events, encouraging good behaviours and habits, and making information easily comprehensible.

Because their markets and regulatory frameworks are more developed and sophisticated, developed nations have dedicated more resources and energy to increasing user awareness. For instance, the EU's EBA has developed standards for IPS security measures and initiated a public awareness campaign regarding payment security concerns (Laleh & Azgomi, 2019:np).

Developing countries face more challenges in enhancing user awareness, as they have less developed financial literacy and digital inclusion (OECD, 2023:np). Moreover, they may lack adequate regulatory models and oversight mechanisms to ensure the transparency and accountability of IPS providers (ACFE, 2020:np). For example, in Africa, where IPS is widely used for Mobile Fraud services, there is a lack of harmonised standards and regulations, which may create confusion and uncertainty. Furthermore, there is a need to address the cultural and behavioural barriers that may hinder the adoption of good practices and habits (ISPA, 2020:np).

Cross-Border Cooperation: To identify, stop, and prosecute cross-border fraudsters, cross-border cooperation which entails exchanging information, resources across many nations and jurisdictions are an essential component of IPS fraud preventions (Button *et al.,* 2017:120). A number of strategies can be used to promote cross-border collaboration, including the creation of networks and platforms for information sharing and coordination, the establishment of common guidelines and standards, and the creation of collaborative projects and activities to fight IPS fraud (OECD, 2023:np). Developed nations have more experience and knowledge handling cross-border payment concerns, and therefore they have developed more sophisticated and all-encompassing models for cross-border cooperation (ISPA, 2020:np). For instance, the EU has many mechanisms for cross-border collaboration between authorities and stakeholders, as well as a high degree of harmonisation and integration of payment systems and regulations (Fisman, & Miguel, 2017:1030). For instance, there is a need to improve the convergence and harmonisation of payment systems and regulations, as well as to fortify cooperation and coordination among stakeholders and authorities, particularly Asia-Pacific, where IPS are increasing quickly (Ferguson, 2017:87).

Investments in state-of-the-art systems should be supplemented by best practices (ISPA, 2020:np):

- Incorporating ‘privacy by design’ and implementing best practice cybersecurity frameworks to strengthen systems will act as a barrier to identity theft;
- The prevalence of damages from identity thefts will be reduced by increasing industry actors' cooperation to exchange almost real-time information on data breaches and related incidents (according to data privacy rules);
- Proactively educating customers on the latest techniques being used by fraudsters to steal identity information will alert customers not to reveal personal information; and
- Reporting data breaches (providers) and identity theft (customers) immediately to law enforcement agencies will limit exposure.

A typical precondition to more serious illegal behaviours like SIM swapping fraudulently is identity theft. Given that identity theft frequently precedes other frauds, it is crucial to examine both identity theft and related frauds simultaneously to reduce the risks involved (OECD, 2023:np).

ISPA (2021) annual report highlights that the following recommendations will play an important part in mitigating risks of SMS fraud

- It should be standard procedure to inform and raise awareness among consumers about the importance of protecting personal information (such as name, date of birth, address, and PIN); for example, by sending out SMS reminders and posting warning signs at agent locations;
- Advising clients on what to do in the event that their personal information is compromised, such as reporting the incident to the police and contacting the financial service provider or Cell-Carrier.
- Agents and staff should go through frequent testing, training, and observation to ensure that they do not t unintentionally reveal customers' personal information. Improved personal information protection measures, including the four eyes principle, should be reflected in systems and policies; providers should work together to provide law enforcement authorities with capacity building and training so they can respond to such situations quickly; and
- In high-risk regions, providers should prioritise investing in local SMS firewalls to enable them to identify and resolve fraudulent activities committed through bulk SMS campaigns via international SMS gateways. In high-risk regions, providers should prioritise investing in local SMS firewalls to enable them to identify and resolve fraudulent activity committed through bulk SMS campaigns via international SMS gateways.

To supplement existing efforts, the SABRIC annual reports from 2018/2022 make the following recommendations

- SIM swaps should be completed at the mobile operator's sales centre with appropriate due diligence in nations where there is a high risk of SIM swap fraud (ACFE, 2021:np):
- Only authorised dealers should do SIM swapping in situations where this is not practical or in nations where the risk is minimal. In this instance, it would be appropriate to impose a 48-hour limit on access to the mobile money account and any other associated financial services accounts;
- Customers should be asked to present identification documents in nations where national identity registrations and SIM registrations are mandated (OECD, 2023:np). Prior to issuing a replacement SIM card, they ought to be verified. In the event that such authentication methods are unavailable, fraudsters should be discouraged by taking a customer's picture;
- Together, financial service providers and mobile operators should create a system for proactively exchanging SIM swap-related information without jeopardising client privacy (OECD, 2023:np). Every time a SIM is replaced, this should involve exchanging static notifications and Internal Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) data. The telecoms regulator should make sure the IMSI data is made available to pertinent stakeholders for free and in compliance with data protection laws;
- Regulators should encourage creating and sharing a watchlist of identified perpetrators of fraud among mobile operators and financial service providers (while respecting data protection laws) to help others identify possible fraudulent activity (OECD, 2023:np). Those on the watchlist should also be reported to law enforcement agencies.

Fraud poses a constant threat to SABI. Protecting SABI customers from fraudulent activities is crucial for safeguarding assets, reputation, and overall operations (Murimbika, 2024:3901). The aim is to provide a comprehensive understanding of fraud prevention and its significance in SABI. Bishop (2022:66) suggests an exploration of various fraud risks in the SABI face and the measures they can implement to mitigate the threats effectively; from anti-fraud policies to cutting-edge software solutions leveraging artificial intelligence and machine learning to uncover the tools and strategies that would empower SABI to detect and thwart fraudulent threats. Fraudulent activities come in various forms, ranging from all types of financial fraud such as account takeover fraud to identity theft, phishing, and card skimming (Ambashtha & Kumar, 2023:101). These schemes can lead to significant financial losses and irreparable damage to a company’s reputation. However, with a robust fraud prevention approach in place, SABI can proactively protect themselves and their customers.

Dawson (2015:16) states that by implementing anti-fraud policies and procedures, companies can establish a framework for identifying and addressing potential threats. Furthermore, leveraging advanced technologies such as artificial intelligence and machine learning enables SABI to analyse vast amounts of data, detecting patterns and anomalies indicative of fraudulent activity (Burrell, 2023:32). The Faster Payments Service (FPS) enables immediate payments, at times in up to two hours if the receiving bank or building society also uses the service and the amount is within the limit (Button *et al.,* 2017:59). The first real-time payment system in the world was introduced in 2018 by the FPS in the UK. Customers can use a variety of channels to send and receive up to R250,000 in a matter of seconds. P2P, bill, online, and business payments are all effected frequently (Vijayan, 2014:np). Authorised Push Payment (APP) and account takeover are the two primary forms of fraud that FPS deals with Authorisation to Operate (AO). APP fraud refers to duping bankers into sending money to scammers. On the others hand, theft involving thieves breaching into consumers' accounts and making unauthorised payments is known as ATO fraud. According to Ferguson (2017:88), the UK has a multi-pronged strategy to fight fraud, including transaction monitoring and analytics, customer education and awareness, Confirmation of Payee (CoP) services, and fraud reporting and compensation.

The subject to fraud related to phishing and social engineering, wherein clients are deceived or coerced into divulging personal information or paying money. (ACFE, 2019:np) Sweden uses a multi-pronged strategy to fight fraud, including SCA requirements, transaction monitoring and analytics, customer education and awareness campaigns, fraud reporting, and reimbursement (ACFE, 2019:np). With a Virtual Payment Address (VPA) connected to a bank account, India's Unified Payments Interface (UPI), which was introduced in 2016, allows for real-time payments up to 100,000 International Normalised Ratio (INR). Payments between peers, internet, and merchants are its primary uses. Phishing and vishing fraud, in which victims are tricked or contacted by con artists, are threats to UPI (Zinn & Dintwe, 2015:88). Like many countries, India has a multi-pronged strategy to fight fraud, including fraud reporting and reimbursement, SCA and device binding, transaction monitoring and analytics, and customer education and awareness (Adekanya, 1986:57; ACFE, 2022:np).

Launched in 2021 in Nigeria, Next-Generation Networks (NGN) allow payments of up to 10 million to be made in real time using a phone number or bank account (Adekanya, 1986:61). Nigeria has a multi-pronged strategy to fight fraud, including fraud reporting and reimbursement, SCA and device binding, transaction monitoring and analytics, and customer education and awareness (OECD, 2023:np) which presents a compelling illustration of the opportunities and difficulties related to deploying digital identity systems throughout Africa.

Nigeria, which had a population of approximately 221 million (June 2023 statistics) and a varied socioeconomic environment, experienced an evolution of identification systems from 2005. This period was characterised by claims of corruption, inadequacies in infrastructure, and privacy issues. But in cooperation with other stakeholders, the Nigerian government has shown a renewed dedication to using digital technology to expedite identification procedures, combat poverty, and enhance service delivery (PASA, 2016:np). The banking subject matters experts in forensics provide a more reliable way to identify and confirm people, lowering the possibility of incorrect or insufficient. According to a World Bank report (PASA, 2016:np) digital identity systems can greatly increase the precision and consistency of identification procedures by employing cutting-edge technology for document verification and analysing meta-data from digital channels, such as Global Positioning System (GPS) location or mobile device data. The OECD (2013:np) digital identification systems are consistent with the idea that identity management is a continuous process that involves updating a person's profile on a regular basis through a variety of data sources. This dynamic approach, known as identity proofing, ensures that identities remain accurate and up to date, allowing appropriate risk-based anti-mobile fraud and counter-terrorism financing controls to be applied (PASA, 2016:np).

A digital identity system has enormous potential for addressing financial inclusion challenges (Open Data Charter, 2018:np). By automating the onboarding process or substituting digital verification techniques like GPS technology for address verification for physical documentation, these solutions can lower costs and increase accessibility (Ojo & Adewanmi, 1982:78, also OECD, 2013:np). This illustrates the revolutionary power of digital identity in boosting financial inclusion. It is evident from delving deeper into the Nigerian context and examining the possible advantages and disadvantages of digital identity systems that this shifting environment calls for a careful balancing act between technological advancements, regulatory models, privacy concerns, and social inclusivity (Laleh & Azgomi, 2019:np). A number of services have attempted to link the National Identification Number (NIN) to a complete system. General Multi-Purpose Cards (GMPC) and unique NINs are issued to citizens and lawful permanent residents by the National Identity Management Commission (NIMC), which also establishes a national identity database (AGSA, 2022:np). With the goal of expediting the identification process and offering a consolidated platform for government services, the NIMC seeks to replace the disjointed ecosystem of numerous identity programmes run by various organisations, such as 9 mobile, access bank, access solutions limited, and others.

This action tackles issues with data security, effort duplication, and inefficient service delivery (SABRIC, 2022:np). Nigeria wants to create a complete digital identity system in order to enhance social and economic development, law enforcement, government, and citizen access to basic services (OECD, 2013:np). By integrating the NIN with SIM cards and banking processes, fraud is prevented, and security is enhanced. Nigerians place a high value on digital identity systems because they facilitate identification procedures, enhance service delivery, and open the door to inclusive growth and effective governance (OECD, 2013:np). According to Delamaire, Abdou, and Pointon (2019:61) there are primary obstacles used in fraud protection in (IPS) as well as potential countermeasures. Researchers have observed that IPS fraud prevention is a dynamic and complicated problem that calls for creative and cooperative solutions from many nations and stakeholders (ACFE, 2020:np). Scholars have also juxtaposed and analysed the various strategies employed by industrialised and developing nations, emphasising their advantages and disadvantages as well as shared objectives and difficulties (Priezkalns, 2019:np; Adekanya, 1986:87). In order to combat fraud in IPS more effectively and efficiently, researchers have highlighted the significance of finding out synergies and alliances, as well as learning from each other's experiences and best practices (Priezkalns, 2019:np).

6.4 THE FORENSIC INVESTIGATION FRAMEWORK MODELS TO COMBAT MOBILE FRAUD

This section presents the forensic investigation framework models that may assist investigators to respond to assertions of fraud and build solid cases. These models, often used in digital forensics, provide a structured approach to gather and analyse evidence, eventually ministering in the prosecution of fraudsters. An analysis ensures that data are accessible and aid in the identification of fraudulent activity. Fraud has long been a serious problem in a variety of industries, including banking, healthcare, insurance, and many more (Coppolino *et al.,* 2015b). Fraudulent activities have expanded as a result of the rise in online transactions made using various payment methods, including credit/debit cards, mobile phones, among others (Boorman & Ingves, 2019:43). Furthermore, thieves and scammers have improved their abilities to steal more. PwC (2022:np) claims that creating a secure system for authentication and guarding against fraud has become a difficult challenge because no system is perfect and there are always loopholes (Coppolino *et al.,* 2015b). Thus, fraud detection systems play a critical role in stopping fraud.

6.4.1 Supervised Learning Used in Fraud Detection Algorithms

Labelled outputs are used to train supervised learning models. A transaction is labelled 'fraud' if it is thought to be an unlawful or dishonest activity, such as when someone is trying to use a payment method without authorisation, whereas a transaction is labelled 'non-fraud' if the payment is approved by the legitimate owner. (PwC, 2022:np). To train the supervised learning model so that it produces a valid output, a significant amount of such labelled data is fed into it. Additionally, the degree of data organisation affects how accurate the model produces results (Castillo, 2009:56).

- **The statement by INTERPOL (2020:np) indicated key points about transaction classifications:**
  - A transaction is usually classified as either 'fraud' or 'non-fraud' in fraud detection systems due to the fact that this is a binary decision-making process.
  - Fraudulent activity: This can involve using a credit card number that has been stolen, buying something from an odd place, or completing a big, unexpected transaction that is out of the ordinary for the account holder's spending habits.
  - Normal purchases made by the authorised cardholder are referred to as non-fraudulent activity.

6.4.2 Unsupervised Learning Used in Fraud Detection Algorithm

Unsupervised learning models are built to detect unusual behaviour in transactions which have not been detected previously (Coppolino *et al., 2015*b). Self-learning is a component of unsupervised learning models, which aids in uncovering transactional patterns. In this kind, the model looks for patterns and distinctions in the transactions that occur, analyses the data that is accessible, and attempts to learn on its own. This aids in the identification of fraudulent activity. Therefore, for the purpose of identifying transaction abnormalities, both models supervised and unsupervised can be applied singly or in combination. Costumers are constantly looking for tools, processes, or strategies that require less work on their part to do a task quickly and effectively (Castillo, 2009;87; Coppolino *et al.,* 2015a). Algorithms in machine learning are created in a way that tries to learn on its own by drawing on prior knowledge. After learning from the past experience, the algorithms become quite capable of reacting and responding to conditions for which they are not explicitly programmed. Therefore, machine learning is quite helpful in detecting fraud. It looks for hidden patterns that aid in the detection of fraud that has not yet been identified. In addition, it computes more quickly than conventional rule-based methods (Sharma & Panigrahi, 2013:40).

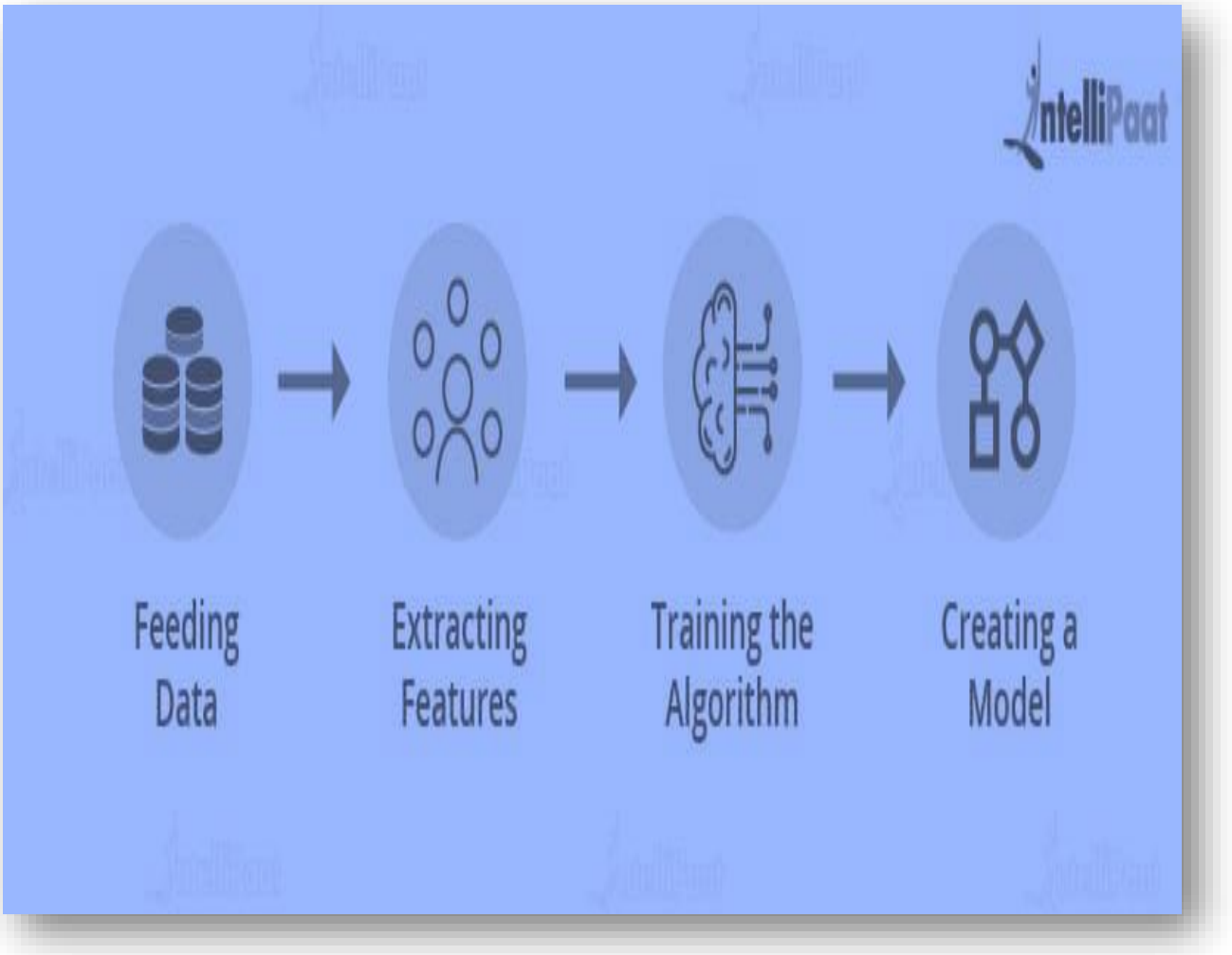
6.4.3 Factors explaining why Machine Learning techniques are so popular and widely used in industries for detecting frauds

- ***Speed***: Because machine learning computes quickly, it is widely used. In a short period of time, it examines, analyses, and finds new patterns in data. Given the volume of data, evaluating it by hand would take longer. Rule-based fraud prevention systems are built on rules that outline what behaviours are permissible and what should trigger red flags (Sharma *et al.,* 2013:41). The rule-based approach is inefficient since writing the rules for many scenarios takes a long time. That is precisely the aspect at which machine learning-based fraud detection systems excel in automatically identifying new trends in addition to learning from existing ones. Furthermore, it completes all of this in a fraction of the time needed compared to these rule-based systems.

- ***Scalability***: The machine learning-based model improves in accuracy and predictability as more and more data are added to it. Sharma *et al.,* (2013:44) indicated that rule-based systems never develop on their own; instead, the experts who created them have to set the rules to account for different scenarios. However, to ensure that algorithms based on machine learning are operating as intended, a committed group of experts in data science needs to be involved.

- ***Efficiency***: Machine learning algorithms carry out the repeated work of analysing data and look for hidden patterns. Their effectiveness in producing outcomes surpasses that of manual labour. Its effectiveness is based on its ability to prevent false positives (Sharma *et al.,* 2013:44). Fraud detection experts could now concentrate on more sophisticated and complicated patterns, leaving the low- to moderate-level issues to these Machine Learning-based algorithms, thanks to their effectiveness in identifying these patterns.

Figure 6.3: The Fraud Detection Algorithms Machine Learning



Sources: Coppolino *et al., (*2015b)

The following model applies to prevention of mobiles fraud:

***Feeding Data*:** The model is first fed with the data. The quantity of data used to train the model determines its accuracy; the more data used, the better the model performs. An increasing amount of data must be entered into the model in order to identify scams unique to a given firm. By doing this, an investigative model would be trained to recognise signs of fraud.

***Extracting Features*:** In essence, feature extraction gathers data from each thread connected to a transaction process. These include the transaction's point of origin, the customer's identity, the payment method, and the network that was utilised.

- ***Identity*:** This element is used to verify a customer's mobile number, email address, and other information. If the consumer requests for a loan, it can also verify the bank account's credit score.
- ***Location*:** It verifies the customer's Internet Protocol (IP) address, shipping address, and fraud rates at those addresses.
- ***Mode of Payment*:** It checks the cards used for the transaction, the name of the cardholder, cards from different countries, and the rates of fraud of the bank account used.
- ***Network*:** It checks for the number of mobile numbers and emails used within a network for the transaction.

***Training the Algorithm*:** After developing an algorithm for detecting fraud, investigators must train it with client data so that the system can learn to differentiate between 'fraud' and 'genuine transactions.

***Creating a Model*:** Once investigators have trained fraud detection algorithms on a specific dataset, they should be ready with a model that works for detecting 'fraudulent' and 'non-fraudulent' transactions in businesses.

When someone intentionally misrepresents the truth or conceals a material fact in order to coerce another person into acting against his/her best interest, fraud is then considered a crime (ACFE, 2022:np). Money transfers, including sending and receiving payments using a mobile device are included in a mobile money service. The GSMCA has developed standards for mobile money services. In order to make the service broadly available to everyone, it must provide a network of physical transactional sites, which may include agents in addition to bank branches and ATMs. The agent network needs to be bigger than the official outlets of the service (ACFE, 2022:np). The unbanked, or those without access to a formal account at a financial institution, must be allowed to use the service. These do not include mobile banking or payment systems (like Apple Pay and Google Pay) that use a mobile device as just another way to access a traditional financial product. Consequently, fraud that occurs on assets owned or held by a mobile money service provider to the prejudice of that provider, its clients, agents, or third parties can be classified as mobile money fraud (ACFE, 2022:np). Money, knowledge, and intangible assets like a company's name, standing, or offerings are examples of assets. Particularly in poorer nations, mobile fraud is a relatively new phenomenon in payment systems. The process of electronically transferring (wiring) goods with monetary value between one or more receivers, the sender and the recipient, is known as mobile fraud.

Mobile fraud has become increasingly popular throughout Africa. Mobile fraud services, sometimes known as digital money, carry some of the same risks as other electronic platforms (Forte, 2013:13). Cybercriminals now use the e-Platforms as a playground for phishing and other financial crimes.

Financial crime is classified as financial abuse crime when the victim loses money, but the crime is not violent in prevalence. Tax evasion and mobile fraud are two examples of financial crime.

- **Mobile fraud is attractive to the criminals because of the following risks:**
  - Speed at which funds are transferred;
  - Lack of physical contact;
  - Ability of layering multiple transactions in small margins.

Risks associated with mobile fraud make it difficult to acquire banking services and use technology. Data security, mobile fraud, and financial fraud are among the threats that must be controlled (Realini, 2021:np). The instruments for identifying fraud related to mobile commerce are out of date. Tools for detecting fraud that worked well in wired networks do not operate as well in mobile environments (National Treasury, 2020:np). In order to combat the conventional and new threats posed by the new payment methods, it is necessary to investigate the various strategies for combating financial crime and provide a fresh approach (Button *et al.,* 2017:111). The hazards associated with mobile fraud transactions rise as the market for them does. Attackers who are both skilled and motivated have turned their attention to mobile fraud transactions. There is potential for misuse in areas like mobile fraud.

Overwhelming data makes it challenging to identify frauds quickly (Coppolino *et al.,* 2015a). Due to new payment platforms like mobile fraud and the constantly developing state of technology, financial crimes are increasing (Button *et al., 2*017:128). The use of virtual money to pay for services through mobile fraud is known as mobile fraud transfer. Particularly in developed nations where the majority of people lack bank accounts, these services have grown in popularity (Coppolino *et al.,* 2015b). Lopez-Rojas and Axelsson (2022:66) claim that the state of research on mobile fraud is not as high as that of other disciplines. Nevertheless, there needs to be protection against mobile fraud.

This study examined mobile fraud as a new payment mechanism and the information technology techniques used by law enforcement to identify and track financial crime. The necessity for a new paradigm for monitoring and controlling mobile fraud transactions was highlighted, along with the limitations of the methods used to detect financial crimes already in use (Button *et al.,* 2017:129). A conceptual model for the detection of mobile fraud transactions was proposed based on an analysis of current models Modern Monetary Theory (MMT). Also proposed are the traits of mobile fraud applications, the sources of the risks associated with mobile fraud, and the ecosystems surrounding mobile fraud. There are strategies for financial crimes involving mobile fraud (Solin & Zerzan, 2010:14).

The conceptual models for detecting mobile fraud and financial crime are some reflections and a conclusion are provided (Chatain *et al.,* 2018:23). They have not been mentioned before so you must write down all the authors.

6.4.4 Mobile Fraud Ecosystem

Tobbin (2021:24) lists partner banks, Mobile Network Operators (MNO), regulators, merchants, consumers, and distribution channels as some of the players in the mobile ecosystem. MNOs, banks, and regulators are among the participants in the mobile fraud ecosystem (Button *et al.,* 2017:143). The facilities and distribution channels needed by subscribers to carry out mobile fraud transactions are provided by the MNO. Agents, or distributors, collaborate with mobile network operators to conduct business on their behalf. Additionally, some merchants engage in remittances. Distribution channels typically serve as a point of contact for consumers who use cash-in-cash services and customer registration (Tobbin, 2021:54).

Most strategies focus on using data mining techniques to combat mobile fraud. The models under study primarily address credit card theft and traditional banking. Because mobile fraud is still in its infancy, only few models focus on it (Button *et al.,* 2017:147). Nonetheless, a literature review in the literature analyses indicated that several ideas are transferable to both traditional banking systems and financial crime detection techniques (SABRIC, 2021:np). Regulations controlling financial crime in the banking industry were developed by the Financial Action Task Force (FATF), which was established in 1989 (Tobbin, 2021:56). These suggestions have been updated on a regular basis as criminals devise new ways to evade established protocols. The FATF 2012 recommendations represent the most recent updates. The proposals do support the use of policies to address the risk of criminality in the financial sector. Additionally, suggestions are provided for employees in Know Your Customers (KYC). Nonetheless, it is incumbent upon nations to adopt these FATF proposals and rules.

Models of data mining system for anti-mobile fraud: A mobile fraud detection model is used in mobile fraud detection models to link the disparate and evolving schemes. The models offered include electronic money (E-Money) for identification through algorithms and suspicious trail databases in SABRIC (Malady, Buckley & Arner, 2014:38). The models of data mining system for anti-mobile fraud are comprehensive models that address a wide range of topics, including mobile fraud. In SABRIC models, investigators or subject matter experts were only scaling down on mobile fraud and not covering other monetary transactions such as traditional banking (Button *et al.,* 2017:133).

Fraud profiling conceptual model: Brungs, Winchester, Stephens and Smith (2018:268) developed a model for detecting fraud. This model examines the process of profiling by means of message forwarding and notifications to various studies. Certain policies kept an eye on activities, profiles, biometric information, identification data, PINs, and key loggers (Button *et al.,* 2017:66). Certain profiling ideas might be helpful in our models since they reduce the possibility of anonymity and improve Customer Due Diligence (CDD) and KYC.

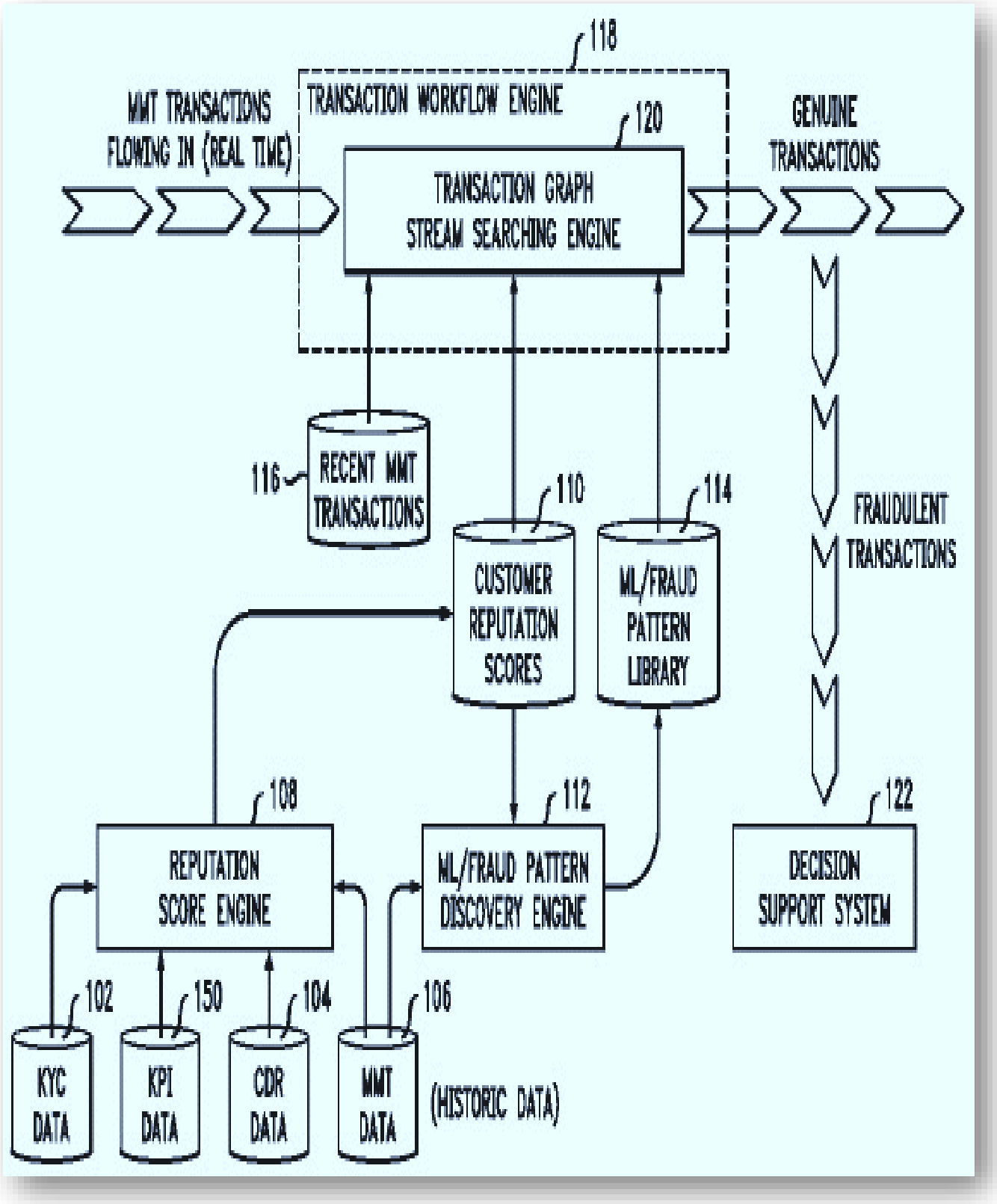
Accounting Fraud Detection: The model for the identification of financial accounting fraud investigates the application of data mining techniques in accounting and financial statement fraud (Sharma *et al., 2013*:43). Accounting Fraud Detection models was to identify outliers and provide rare pattern visualisation (Tobbin, 2021:77). The models were predicated on the idea that outlier detection techniques could be used to differentiate between real and fake data, and that data anomalies might be displayed using visualisation techniques (Sun, Srivastava, Mock, 2016:22). Although some of the approaches, particularly the outlier identification methodology, can be utilised to combat mobile fraud, the model's design is appropriate for traditional banking models (Brungs *et al.,* 2018:57). Care should be exercised, though, as thieves can utilise the summering approach to get around the detection of outliers by transacting different amounts to several clients using numbers below the threshold. In the face of newly developed payment options, this tactic needs to be used in conjunction with other strategies (ACFE, 2022:np).

Time Series Data Set architecture: This refers to mobile fraud that uses a multi-variant model based on transactions set to detect proceeds of financial crimes. The pre-processing of transaction data logs by deleting incomplete log data is described in the literature of this study. By separating separate accounts from unique accounts, relational mapping must be used to verify these data transactions (ACFE, 2019:np). A one-to-many relational metric check was performed on the accounts data. Next, a generalised format was created using the patterns that were extracted from the log. After conversion, the data was sent for the purpose of identifying mobile fraud (Button *et al.,* 2017:136). A time series data of the transaction data will be performed in the mobile fraud identification by splitting data performed at a specific time frame. The total amount transferred from one- to- many, or many- to- one relationship was then calculated using threshold values. A set of rules was created to determine whether a transaction qualifies as suspicious if its total value exceeds a predetermined threshold (Prabakaran, 2014:44). It can be used to identify fraudsters who divide up major transactions into smaller ones or who use mules.

A criminal can deposit money into an account and send it through a chain of transactions. In this many-to-one sort of financial fraud, criminals who con individuals into pyramid schemes or who sell houses to several home seekers can be identified (ACFE, 2022:np). Time Series Data Set architecture is employed to identify and keep an eye on transactions that may be deviating from established guidelines for lawful transactions. The system verifies client risk in the models and adds a risk to the transaction by assigning a severity level (Button *et al.,* 2017:138). A risky score and a suspicious mark are applied to a transaction if one of the studies determines that it is suspect. The transaction passes through the monitoring phase which contains many studies such as rule base, feature detection, cluster, cycle detection, and suspected link monitors (Batra, Garg, Kothari, Krishnapuram, Negi & Parija, 2013:81). According to the models, a customer's due diligence results in the risk being assigned to them and their transactions.

The above-mentioned authors suggest that, in the event that a client transfers money to a suspect, the transaction is considered suspicious based on a suspect connection analysis that conceals hidden relationships, such as those with individuals on a sanction list or those notified by the government (ACFE, 2022:np). The models also provide for cycle detection where money transferred through layering is returned back to the initiator (Batra *et al.,* 2013:111). Any suspicious transaction is examined in the historical databases. This model is crucial to suggested models since it allows the investigators to classify clients as dangerous and utilise a suspect link analyser. For instance, criminals with prior convictions may be designated as dangerous clients, and any transaction they complete is considered questionable. The models can also be utilised to identify suspects who wish to introduce and withdraw illicit funds under the guise of genuine currency by using cycle detection (ACFE, 2022:np).

Figure 6.4: Models for Detecting Fraudulent Mobile Fraud Transaction



Source: Batra *et al.,* (2013:113)

Luo (2014:107) presents a data mining approach for combating mobile fraud in which transactions are cleaned, converted, and analysed for data mining purposes. The knowledge gleaned from these processes is then stored in a knowledge base for use in recommended systems and visualisation. The models concentrated on a classification-based algorithm-based dynamic detection method for suspicious transactions using stream data (ACFE, 2022:np). The speed at which transactions are completed indicates that the models were not well matched to the mobile fraud ecosystem. On the other hand, suggested models may benefit from a knowledge base to store newly discovered information.

The models developed by Batra *et al.,* (2013:114) were intended to identify consumer behaviours, classify transactions as authentic or fraudulent, and define a reputation score based on historical data. Reputation was also used to identify multiple patterns connected to fraudulent mobile fraud transfer. The models detect abnormal mobile fraud transfer transactions in order to identify potential hazards and attempt to detect fraud in real time. Real-time anomaly detection systems are made possible by the models to spot questionable transactions. The models provide automated ways to identify patterns in the investigation of mobile fraud. Inactive patterns, call detail records, and the KYC database are also provided by the models. In order to evaluate client usage patterns and automatically classify transactions that may be suspicious of being mobile fraud, the models also incorporate key performance indicators. To identify mobile fraud (MF) or fraud patterns, the data were rated using a reputation score database and customer reputation score. A transaction graph is then used to analyse these (Sun *et al.,* 2016:27). The models do not, however, provide a way to discriminate between legitimate and fraudulent transactions. Since this model can be used to give risk scores and create rules in the ontology study, it was helpful in the creation of this research proposed models. Because it is helpful for maintaining transaction records in line with Financial Action Task Force (FATF) recommendations to retain records for five years, the historical database engine is also suitable in models.

6.4.5 Analysis of the Existing Models

Most of the models under analysis make use of data mining; nevertheless, this technique has limitations in terms of only revealing information that the analyst is looking for, and patterns found may be the consequence of data inconsistencies caused by random fluctuations (Zengan Gao & Mao Ye, 2017:91). Since data mining is labour-intensive and unproductive for covering shifting data, big data analytics can be helpful here. Traditional fraud detection methods primarily focused on the identification, validation, and client profile processes based on historical transactional data. However, they are not very good at spotting possible fraud and insider trading (Zengan Gao *et al.,* (2017:93).

There are several obstacles specific to data mining, including noisy data, difficulty tracking user behaviour, and frequent changes in behaviour. Furthermore, extremely effective strategies are required for obtaining enormous volumes of data (Singh & Singh, 2015:77). Based on the various methods and models for detecting financial crime in mobile fraud, the imaging challenge calls for a holistic approach to uncover hidden risks in mobile fraud. Tackling financial crime is a challenge because a lot of internal control systems have serious control weaknesses. However, its key aspect is the ability for technology to maintain comprehensive logs of all performed activities and electronic transactions of fraudulent activity or heightened fraud risk (Dzomira, 2014:116). Cybercriminals are aware that banking financial detection systems seldom keep track of customers' actions across several accounts, channels, and systems; a shortcoming which makes cross-channel financial crime easier to do. A fraudster obtains customer information through one channel, which they then use to perpetrate fraud through another. Furthermore, it is more challenging to identify fraudulent communications and covert interactions due to the anonymity of e-commerce (Albshaier, Almarri & Hafizur Rahman, 2024:27).

6.4.6 Proposed Conceptual Models for Mobile Fraud Detection

(Albshaier *et al., 2024*:27) state that automated financial crime relies on mobile fraud trends and the network for alleged mobile fraud, but traditional online financial crime research has focused on compliance and legislation. The techniques are restricted to identifying incidents and detecting suspected surveillance avoidance, and the investigations are laborious, time-consuming, and largely manual (ACFE, 2018:np). When high-volume sets are present, the existing approaches cannot effectively handle false positive rates and become invalid (Zengan Gao *et al.,* 2017:139). The models use big data analytics, which examines enormous amounts of data that deals with diversity and noise removal. The velocity of the data refers to both the speed at which the data is generated and the real-time environment. Value extraction from the data is necessary because of the millions of transactions that financial fraud transactions create. When a legitimate transaction is mistakenly identified as illegal, legal action may follow; conversely, when an illegal transaction is mistakenly identified as legal, business may be lost, and financial crime may be encouraged (INTERPOL, 2020:np).

The suggested conceptual frameworks for identifying financial crimes involving models for detecting fraudulent mobile fraud transaction are shown in Figure 6.4. The models cover surveillance tasks like social network analysis, mobile fraud, and fraud. Through the usage of models of mobile fraud platforms and their criteria, the models also incorporate the early observations and suggestions from the FATF from 2012.

Given the fact that financial crime is dynamic, the Financial Intelligent Unit (FIU) and investigative authorities need to take a comprehensive approach to use automated methods to detect financial fraud. When a transaction is considered suspicious, it may not always be so, and vice versa. Therefore, caution should be exercised in correctly identifying suspicious transactions. These models explained in this research can assist the FIU and investigators in identifying characteristics that are hidden in mobile fraud transactions. The models will process data from a variety of information sources. The various data will be placed in an MF for cleaning and pre-processing. MF files convert files to a common format, and they are not specific to any database.

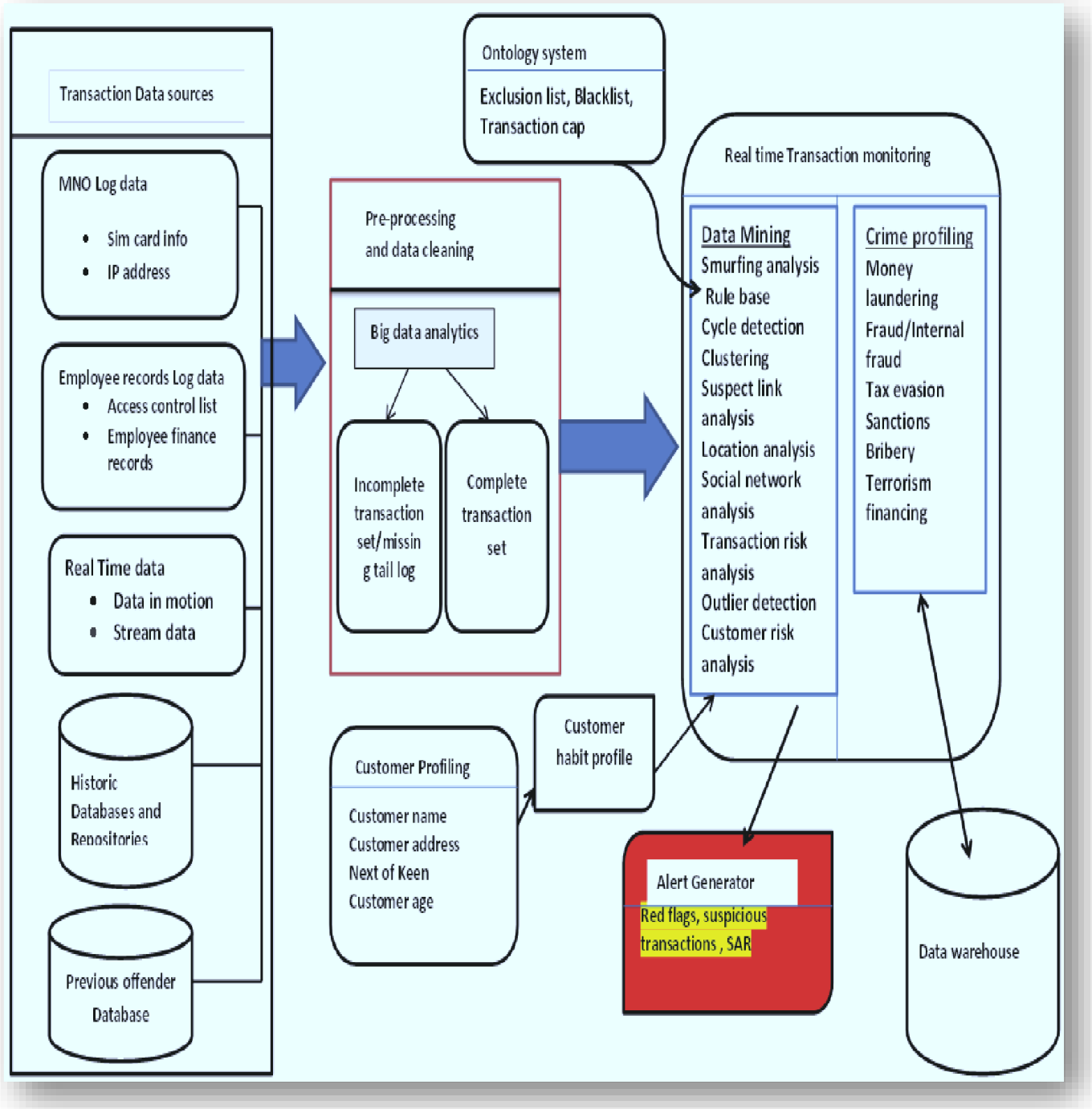
The majority of the data comes from MNO log files, which contain information about SIM cards, SIM card replacements, and SIM registrations (AGSA, 2022:np). The MNO's network would generate most of the agent data, but MNO databases would store the data. Pre-processing would make use of this data. Data from employee records would be utilised to track their access rights and the sessions they checked in to. Employee information may also include statements about their assets and net worth. Successful and unsuccessful transactions would be cleansed for processing from transaction data that is currently in motion. Committed transactions and previous transaction records can be found in historical data and repositories. Banks and other financial institutions are required by the FATF to retain transaction data for a minimum of five (5) years. A list of offenders who have previously been found guilty of financial crime or issued warnings would be available in the previous offender database (SABRIC, 2022:np). This includes those who have been placed on a banking industry blacklist and those who were previously thought to have committed financial crimes but were ultimately found not guilty.

Pre-processing: The data gathered from the data collections would be cleaned to check for incomplete and noise transactions. Big data analytics tools can be used since the data might be in motion as well as the data being voluminous. The transactions that are complete are then forwarded for monitoring.

Ontology System: The ontologies are purposeful models that are domain-related and created to contain knowledge or information that must be shared. Declarative formalism uses collections of objects to represent knowledge and describe the relationships between them (Gruber, 1995:913; Rajput, Khan, Larik, & Haider, 2014:54). According to Trausan-Matu and Neacsu (2018:66), ontology can also be thought of as a knowledge-based system that makes use of a declarative knowledge base that contains the ideas and relationships that are present in a certain domain. An ontology study can be used to specify rules for threshold values, exclusion lists, and transaction caps that will be used during transaction monitoring. Rajput, *et al.,* (2014:66) ontology is utilised in the development of expert systems since it offers a clear definition of knowledge and can adapt to a changing knowledge base.

In addition to domain knowledge, the ontology-based expert system includes some rules to aid in reasoning. This study is useful for link analysis, outlier detection, and rule bases. The ontology engine specifies the sets for outlier detection, customer ranking, and exclusion lists. The ontology system engine contains the set of rules for distinguishing between legitimate and questionable transactions.

Figure 6.5: Conceptual Models for Detection of Mobile Fraud



Source: Coppolino *et al.,* 2015a)

Real Time transaction monitoring: The majority of detection techniques and technologies are passive in prevalence. The study in this suggested model instantly looks for transactions that seem suspicious. Various offences can be verified using data mining techniques, such as clustering, suspected connection analysis, location analysis (where the system looks up the suspect's whereabouts), and customer behaviour (Rajput *et al.,* 2014:71). A transaction would be profiled based on the probability of the variable and rank if it was thought to be suspicious. Panigrahi, Kundu, Sural, & Majumdar (2007:55) many-to-one transaction, for instance, could point to the commission of fraud, such as pyramid schemes or the sale of a single home by a real estate agent to numerous buyers. The statement by Coppolino *et al.,* (2015a) indicates that for any transaction conducted and linked to a blacklisted person, the said transaction would be categorised as suspect.

- **Alert Generator**

When a transaction is likely to be suspicious while the system is keeping an eye on it, it is sent to the alert generator for suspicious activity and red flags.

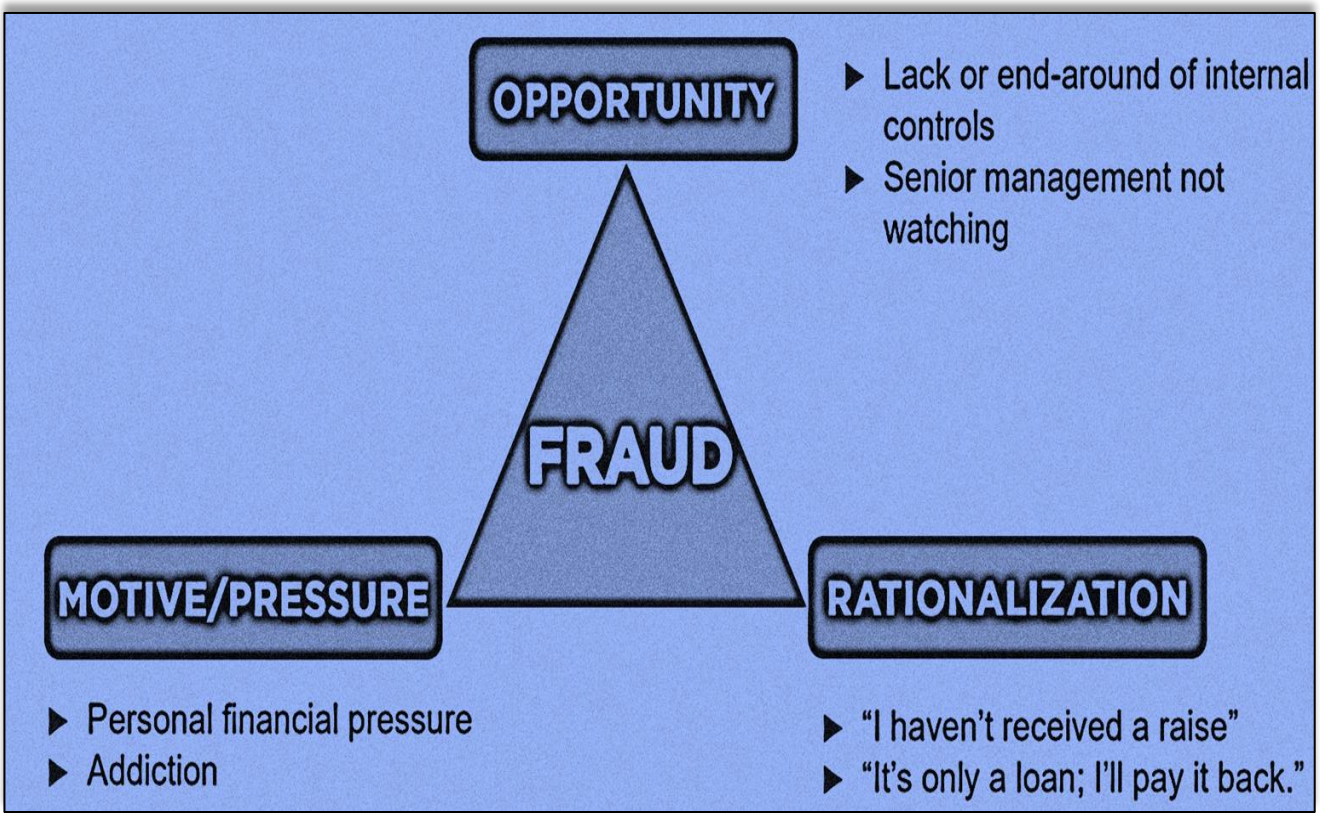
- **Customer Profiling**

CDD and KYC policies will take advantage of this. Social network research and an understanding of consumer behaviour can both benefit from the profile data. Link analysis can be used to find suspicious linkages, analyses patterns of behaviour in interactions, and reveal hidden groups (Marakalala, 2023:29).

- **Data Warehouse**

Since monitoring generates a lot of data, it is best to store the data in a data warehouse for further analysis. The Dempster-Shafer theory is utilised to infer data, and the data warehouse is required to store heterogeneous data sources. Evidence is also combined using the theory (Yager, 1987:43; Panigrahi *et al.,* 2007:144). The theory can be used to avoid unwanted results, for example separating genuine from illegal transactions in the proposed models (Coppolino *et al.,* 2015a).

Figure 6.6: The Fraud Triangle



Source: Donald Cressey (Cressey, 1953 Turvey, 2013:34)

The fraud triangle is an effective model for analysing the SABRIC annual statistical reports susceptibility to fraud and unethical behaviour. Businesses could minimise fraud and other unethical behaviour if they concentrate on preventing each element (Coppolino *et al.,* 2015b). Additionally, the theory helps to explain who is more likely to commit fraud as well as the conditions that made fraud more likely (Cressey, 1953:66). This could assist organisations in concentrating their anti-fraud strategies in specific domains. For instance, fraud is more likely to happen when internal controls are weak or ineffective, as they often are in the early phases of project or process development when controls are tailored to the mobile cycle or when controls are few (Labuschagne, 2015:263). If duties are not assigned appropriately or if there is inadequate supervision of agreements or transactions throughout the bidding process, for example, there may be a risk to the integrity of controls throughout the mobility cycle due to a lack of resources (Turvey, 2013:88). However, this could be lessened by organisations having forensic and internal audit departments that are properly staffed, as well as by knowing and understanding the fraud triangle and the factors that drive fraud, particularly mobile fraud (Lokanan, 2015:65). There is no single reason behind fraud and any explanation of it needs to take account of various factors. Looking from a fraudster's perspective, it is necessary to take account of:

- The reasons for possible offenders' actions;
- Circumstances in which individuals can justify potential crimes;
- Chances to perpetrate a crime;
- Beliefs that targets were appropriate for fraud;
- Technical proficiency of the scammer;
- The real and anticipated risk of being discovered after the fraud has been committed;
- Anticipations of the repercussions of discovery (including non-penal ones such as familial stigma and job loss, confiscation of illicit proceeds, and conventional criminal sanctions);
- Real-world effects of the finding.

Motive: Researchers and experts in preventing fraud usually look for financial pressure or incentives to determine reasons. According to Labuschagne (2015:186) the pressure to meet financial targets, for instance, can lead to high levels of pressure to engage in fraud. Examples of such pressure include sending an email containing the reason for the dispute, invoice number, mobile devices applications screenshot, transaction charge details, or a message of deduction to disputes. South Africa suffered greatly from the global financial crisis of 2018/2022, which led to the loss of about 900,000 (net) jobs (SABRIC, 2018:np). The primary consequence of the downturn, especially for black South Africans without formal education, has been a rise in discouragement rather than an increase in official unemployment (Turvey, 2013:88). The main causes of the global financial crisis are:

- Excessive risk-taking when the macroeconomic climate is favourable;
- An increase in bank and investor borrowing;
- Flaws in regulations and policies;
- Debtors failed to make payments;
- Tensions within the financial sector;
  Spill over into foreign nations.

To put it plainly, motivation usually stems from necessity or greed. The annual statistical reports-2018/2022 highlighted that 63% of incidents had a cause mentioned, indicating that greed remains the primary driver of fraud, according to the most recent Fraud Track survey. Debt and gambling-related issues were mentioned as other factors. Only a small percentage of the avaricious and desperate take advantage of the many opportunities to commit fraud. There are factors related to temperament and personality, such as people's level of fear of the repercussions of taking chances.

Even those with sound moral beliefs may end up in the wrong group or circle and acquire a taste for the fast life, which might lead them to commit fraud. Others are only tempted in the face of certain doom.

Opportunity: When fraud is not identified, there are several opportunities for it to happen. SABRIC subject matter experts frequently use internal structural elements, such as internal controls or auditing procedures, to discover fraud potential (SABRIC, 2019:np). A financial crisis or other similar economic conditions may potentially present more chances (Caulfield & Steckler, 2014:41). For instance, there may be more opportunities at a business which makes it more difficult to uphold the separation of duties a crucial component of preventing fraud. Researchers also scrutiny for possibilities, as this can influence how individuals who are inclined to commit fraud calculate their risk (Labuschagne 2015:263; James & Nordby 2018 :65).

Fraud is more likely to occur in organisations with insufficient internal control systems, inadequate security for corporate assets, low levels of exposure fear and discovery probability, or ambiguous policies regarding appropriate behaviour. Many employees are influenced by opportunity, whereas others are completely honest and some are completely dishonest (Caulfield *et al.,* 2014:43).

Rationalisation: The fraud triangle postulates that the ability of employees to rationalise fraud is a third essential element for fraud when chances to commit fraud coexist with motivation. Workers may find it simple to justify fraud, for instance, if they think executives support it or if they think it common practice in the sector (Caulfield *et al.,* 2014:44). Experts in preventing fraud also consider economic arguments that can be used to justify it, such as the notion that committing fraud is essential to a company's ability to weather a financial downturn.

Research by Cressey (1953:66) and Turvey (2013:90) has shown that conditional environmental conditions have a greater influence on individual acts of fraud than they do on intrinsic personality qualities. For this reason, the fraud triangle is a crucial conceptual tool for identifying settings that are favourable to fraud. The SABRIC, AFCE, GSMA, ISPA and AGSA annual statistical reports from 2018/2022 in detecting fraud can pinpoint businesses, sectors, and financial environments that are especially favourable to corruption by noting situations where more pressure or incentives to commit fraud, enough chances for the mobile fraud to go unnoticed, and places where workers can justify their actions (SABRIC, 2022:np).

6.5 SUMMARY

This chapter summarised the challenges encountered by the forensic investigators in the investigation of mobile fraud at SABRIC. The synopsis included scale economies and network effects, the need for a significant amount of capital, as well as an urgent need of consumer switching costs. Organisations are impacted by fraud in a number of ways, including psychological, operational, and financial aspects. The entire impact of fraud on a business can is astounding, apart from the considerable financial loss. The harm to one's good name, relationships with customers, and goodwill can be severe.

CHAPTER SEVEN

PRESENTATION AND INTERPRETATION OF THE RESEARCH FINDINGS

7.1 INTRODUCTION

In this chapter, the researcher described stages involved in collecting and analysing the data consulted and studied for this study. Additionally, this chapter presented the research findings emanating from the six annual reports from 2018 to 2022 that were sampled to answer the questions posed by the researcher during data collection sessions. In that regard, the criticality of the present chapter is underpinned by the interpretation of the research findings which it serves as the most pivotal reference point for the much-needed practical evidence of the study in relation to both the research problem and aim of the study. By implication, the evidence of the study provides extensive details concerning the sampled narrative literature review (annual statistical reports-2018/2022), profound perspectives, knowledge, perceptions, experiences, and thoughts regarding the investigated phenomenon i.e., biometric-based solution in combating mobile fraud at SABRIC annual statistical reports, ACFE annual statistical reports, GSMA, ISPA and the AGSA reports from 2018/2022 (Vithal & Jansen, 2019:65; Creswell & Poth, 2018:47).

This chapter reported on the findings of the study and mapped out the findings in light of the narrative literature review that was analyses in the process of resolving the identified problem of mobile fraud at SABRIC. This research aimed to contribute a biometric-based solution in combating mobile fraud in SABRIC. Following the narrative literature review (annual statistical reports-2018/2022), the chapter continued with a concerted presentation of discussions emanating from the narrative literature review (annual statistical reports-2018/2022), viewpoints, knowledge, thoughts, and understanding regarding the investigated phenomenon of the biometric-based solution in combating mobile fraud under SABRIC jurisdiction.

7.2 EMERGING THEMES PERTINENT TO AN EXPLORATION OF BIOMETRIC-BASED SOLUTION IN COMBATING MOBILE FRAUD

The information obtained through the process of narrative literature review (annual statistical reports-2018/2022) was explored and presented by means of the themes that emerged in the study. This was done to present a detailed discussion of the biometric-based solution in combating mobile fraud at SABRIC. Findings refer to results that are discovered during a research study.

The aim of non-empirical data collection with representatives of the biometric systems providers and experts was to learn more about the current state of biometrics systems at SABRIC and to explore opinions about attitudes and factors influencing adoption/deployment of biometrics systems in the banking sector. Furthermore, the aim was to express experiences, opinions, and domain knowledge about the implementation of biometrics-based solution to combat mobile fraud at SABRIC. The evidence of the study was thematically established in the context of both the research objectives and research questions. It is important to note that these themes serving as the cardinal foundation of the study evidence emerged from the analyses and interpreted content of each narrative literature review (annual statistical reports-2018/2022) as proof or practical evidence of the study's various claims in relation to the core aspects of the research topic (Creswell, 2020:11; Kumar, 2020:66).

This chapter described data that were conceptually developed through published literature (annual statistical reports-2018/2022) with exact assertions acting as the foundation or models for the study's crucial supporting documentation (Yin, 2018:15). As a matter of ethics, the verbatim statements from the narrative literature review (annual statistical reports-2018/2022) were analyses in the study. Additionally, this served to increase the credibility of the findings by guaranteeing that they accurately reflected the genuine perspectives and views (or lived experiences) of the SABRIC annual statistical reports-2018/2022 (Vithal & Jansen, 2019:102). It is extremely challenging for law enforcement agencies to trace the funds when victims are compelled to make payments into banks. Should new regulations be implemented, it would become harder for criminals to evade law enforcement when they employ numerous mobile numbers for illegal activities such as fraud, mobile fraud, terrorism, and kidnapping. Furthermore, consumers would gain an additional layer of protection against identity fraud or unauthorised payment verification through their mobile number since biometric information cannot be duplicated (SABRIC, 2017:np). As highlighted in Section 1.4.1 of Chapter one in this study, the aim of this study was to explore the prevalence, causes, and consequences of biometric-based solution in combating mobile fraud at SABRIC. Consistent with this research aim, the developed themes and consequent findings of the study were generated in response to the following objectives:

- To identify the prevalence of mobile fraud in the SABI;
- To identify the factors contributing of mobile fraud in the SABI;
- To identify the challenges encountered by the forensic investigators in the investigation of mobile fraud in the SABI;
- To establish the best practices by developing a conceptual model to combat mobile fraud in the SABI.

Table 7.1 is a diagrammatic representation of the main or comprehensive 4 (four) themes and the associated sub-themes that emerged from the analyses secondary data collection accruing from the narrative literature review (SABRIC annual statistical reports-2018/2022). As a whole, these themes focus on the identification of den the prevalence of mobile fraud at SABRIC; to explore biometric-based solutions in combating mobile fraud at SABRIC; challenges faced by forensic investigators; banking subject matter specialists; measures to curb and reduce crime such as mobile fraud; as well as society's role in curbing and reducing the high rate of mobile fraud. The Qualitative Data Analysis (QDA) Miner software assisted in the narrative. To identify literature review (SABRIC annual statistical reports-2018/2022) and classifying the data into the below-stated themes.

Table 7.1: Main Themes and Sub-Themes Generated from the Findings

Main/ Global Theme	Category/ Sub-theme	*Sub-Category*
To identify the prevalence and of mobile fraud at SABRIC	▪ Mapping out the challenges that affect mobile fraud at SABRIC. ▪ The prevalence of SIM swap fraud in financial crime ▪ SABRIC's response to biometrics-based solution to combat mobile fraud at SABRIC. ▪ SABRIC's response to mobile-based money transfers allowing users to access financial app. ▪ The need for biometrics-based solution in combating fraud. Mobile payments are growing significantly in developing economies. ▪ To link biometrics-data to combating mobile fraud at SABRIC.	*The prevalence of mobile fraud at SABRIC*
To identify the factors contributing to mobile fraud at SABRIC	▪ Poor/ Inadequate Surveillance Support. ▪ Poor/ Lack of Training Support. ▪ Poor/ Lack of Proper Equipment.	
Avoiding/ Reducing socialising in ATMs and showing of bank card to strangers.	▪ To trace the perpetrators app kidnapping crime of mobile fraud at SABRIC.	
	▪ To effectively combat mobile fraud at SABRIC.	

Researcher Analysis: Main Themes and Related Sub-Themes to Combat Mobile Fraud-2018/2022

The above-stated four main themes and their related sub-themes and categories are subsequently discussed:

7.2.1 Theme 1: The Prevalence of Mobile Fraud in the SABRIC

The research findings were informed by information in published literature as well as in reports, as listed: SABRIC, ACFE, GSMA, ISPA, INTERPOL and the AGSA annual statistical reports from 2018/2022 all of which were used to explore the raw data. After perusal of narrative literature review (annual statistical reports-2018/2022), the following themes surfaced from the SABRIC statements in response to the question: *What are the biometrics-based solution to combat mobile fraud at SABRIC?* Six sub-themes or categories emerged from the above-stated main or universal theme, namely, the researcher established the following about **biometric-based solution in combating mobile fraud** from a review of the narrative literature review and literature review (SABRIC annual statistical reports-2018/2022).

7.2.1.1 Sub-Theme 1.1: Mapping out the prevalence that affect mobile fraud at SABRIC

Mapping out the prevalence of mobile fraud crime is definitely associated with markedly dented SABRIC's data security. Criminals jeopardise SABRIC's clients, digital services, and mobile service providers by utilising counterfeit identities and executing SIM swap fraud schemes (SABRIC, 2019:np). As technology progresses, SIM swap fraud has emerged as a greater concern than it has ever been. The increase in smartphones and mobile applications, along with the ongoing expansion of the mobile industry, has created an increased demand for safeguarding sensitive information (ACFE, 2020:np). Banking applications, online banking, and mobile banking have undoubtedly created a significantly enhanced method for consumers to conduct payments swiftly and effortlessly. Although there is no question that mobile technology will keep advancing, it is crucial to recognise the dangers that advancing technology may bring (Button *et al.,* 2017:98).

7.2.1.2 Sub-Theme 1.2: The prevalence of SIM swap fraud in financial crime

Several financial crimes employ SIM swap fraud as a tactic, because it provides criminals with entry to mobile banking and money transfers as well as transactional verification tokens such as OTPs. SABRIC (2018:np) indicates that the heightened use of banking applications and mobile banking is a significant factor contributing to the rise in mobile banking fraud. One prevalent scheme involves voice phishing or vishing.

According to SABRIC (2018:np), these scams surged dramatically by 200% in 2018, with 11,077. In this scheme, con artists impersonate banking representatives or service providers to deceive consumers into disclosing sensitive information, including one-time passwords or random verification numbers. Emails can also be dispatched to mislead consumers into clicking on a link that permits scammers to acquire banking information (ACFE, 2021:np). Once scammers obtain this data, they can impersonate the victim to request a SIM swap from the victim's mobile network provider. With access to one-time pins and other security notifications, fraudsters can execute transactions swiftly and effortlessly (SABRIC, 2020:np).

7.2.1.3 Sub-Theme 1.3 SABRIC's response to biometrics-based solution to combat mobile fraud at SABRIC

In response to an increase in financial crime associated with SIM swaps, the SABRIC established a deadline that users of active SIM cards had to follow when registering user details. But it has been difficult to get the high adoption rates they had hoped for, along with implementing biometric SIM registration. SABRIC (2018:np) indicates that numerous victims of SIM swap fraud only become aware of their scam when they find themselves unable to connect to their mobile network. Addressing this type of fraud demands swift measures to place a hold on bank accounts and facilitate communication among victims, banks, and mobile network providers. The rise of online and mobile banking, alongside the continual advancement of technology as a whole, has led to a greater complexity in various digital crimes. In terms of mobile banking, it can sometimes be challenging to identify scams like SIM swap fraud. Pickett and Pickett (2002:22) and Lusthaus (2018:88) posit that many network controls and procedures are restricted, with human error and even participation noted in several instances. Banks discover newer and better methods to combat these crimes. Improved authentication procedures are necessary to recognise fraudulent transactions. Technologies such as SIM swap detection present the most effective means of protecting sensitive information, making it simpler for transactions to occur securely (ACFE, 2020:np).

Further details about the consumer are frequently gathered via social media, such as full name, date of birth, or other specifics that can assist scammers in impersonating their victims. After acquiring this information, scammers can impersonate their victims by persuading mobile network operators to cancel or restore their victim's mobile number to their SIM (SABRIC, 2018:np). Subsequently, all messages and calls directed to the victim's phone are forwarded to the scammer – including passwords essential for carrying out banking transactions. This provides fraudsters complete access to their victim's bank account (ACFE, 2018:np).

7.2.1.4 Sub-Theme 1.4: SABRIC's response to mobile-based money transfers allow users to access mobile banking application

SIM Swap detection conducts real-time assessments of customer data, enabling banks to track SIM swaps more efficiently. The likelihood of scams can also be evaluated, facilitating actions such as freezing customer accounts, halting transactions, or broadening the verification process across alternate channels. This might involve several actions, including the following:

- Bank receives a notification that an individual is attempting to add a new beneficiary to an account;
- User tries to add a beneficiary via a mobile banking application;
- Bank sends an advanced push notification to the user's number to finalize the action;
- User confirms the operation with a tap;
- Bank assesses if a SIM swap has taken place;
- Bank subsequently verifies the transaction's legitimacy by sending a security question through a push notification;
- If the user cannot respond to this question, the bank takes additional measures to prevent the scammer from completing the transaction.

7.2.1.5 Sub-theme 1.5: The prevalence of biometrics-based solution in combating SIM swap fraud

Biometrics, particularly facial recognition, offer secure identity verification, preventing fraud and providing certainty that users are who they claim to be. Identity verification is thought to be a method that provides easy-to-use, safe, scalable digital identity verification solutions. These solutions are thought to improve consumer protection and mobile security while also making it possible to access vital resources including financial, governmental, and mobile services. SABRIC uses biometric facial authentication to link SIM cards to real people and stop identity fraud, providing mobile carriers with a full solution. The platform makes sure that applicants are 'live' people by verifying identity documents, RICA information, and face photos. This eliminates the possibility of SIM swap fraud and offers a safe and straightforward onboarding and registration process. Mobile networks must not become complacent regarding SIM swap fraud, and they should prioritise customer protection. According to SABRIC (2020:np), there are minor decreases in reported SIM swap fraud, however, mobile service providers need to enhance their data security to safeguard against fraudsters utilising false identities and SIM swap schemes.

This is especially pertinent as the telecommunications and banking industries grow more interconnected (ACFE, 2018:np). Currently, banks provide mobile services, and mobile network operators offer financial services, resulting in a confluence of the regulatory needs of FICA and RICA. This transition has resulted in increased identity theft threats, necessitating mobile operators to implement rigorous identity verification methods inspired by the standards of the financial sector (SABRIC, 2020:np). Operators must establish practical, robust security solutions that comply with and exceed current telecommunications legislation. To tackle SIM swap and identity fraud, networks should concentrate on delivering straightforward, scalable, and secure digital identity. This has significant implications, not only for safer mobile usage and consumer protection against fraud, but also for consumers' ability to access mobile, financial, and governmental services via their phones (SABRIC, 2021:np). For instance, Vodacom utilise facial biometrics to enhance the SIM card activation process, allowing for quick and secure customer onboarding while adhering to regulations.

7.2.1.6 Sub-theme 1.6: To link biometrics-data to combating mobile fraud at SABRIC

The Independent Communications Authority of South Africa (ICASA) suggested an approach involving connecting biometric data to SIM cards. If implemented, new rules would mandate that all South Africans submit their biometric data to mobile service providers in order to acquire a new cell phone number or perform a SIM swap (SABRIC, 2018:np). ICASA's suggestion includes biometric data types such as fingerprint mapping, facial recognition, and retina scans to be linked to a consumer's SIM card. Government agencies like Home Affairs and Social Development would be able to verify that grants, documents, and other communications reach the appropriate recipient. There are also significant opportunities in the digital payments sector as remote biometrics facilitate access to services that could significantly enhance financial inclusion (Faundez-Zanuy 2016:54). Since most South African adults possess a mobile phone, biometrics alleviates the difficulties in the payment process, rendering transactions straightforward, immediate, and secure (SABRIC, 2019:np).

7.3.2 Theme 2: Factors Contributing to Mobile Fraud at SABRIC

This theme emerged from the narrative literature review (SABRIC annual statistical reports, ACFE annual statistical reports, GSMA, ISPA and the AGSA (reports from 2018/2022) analysis statements in the context of the question: *What are the factors contributing to mobile fraud at SABRIC*? Four sub-themes or categories emerged from the above-cited main or overall theme, namely, research based on the narrative literature review. In that regard, the researcher discovered the following:

- Corruption relating to financial crime;
- Impact of unemployment in the South African society;
- Property crime;
- Income;
- Weak institutional and financial regulatory systems;
- Individual selfish interests;
- Sociopolitical marginalisations;
- Drug trafficking;
- Public fund mismanagement;
- Policy implications.

Examples of **biometric-based solution in combating mobile fraud** information in mobile fraud may include the following information:

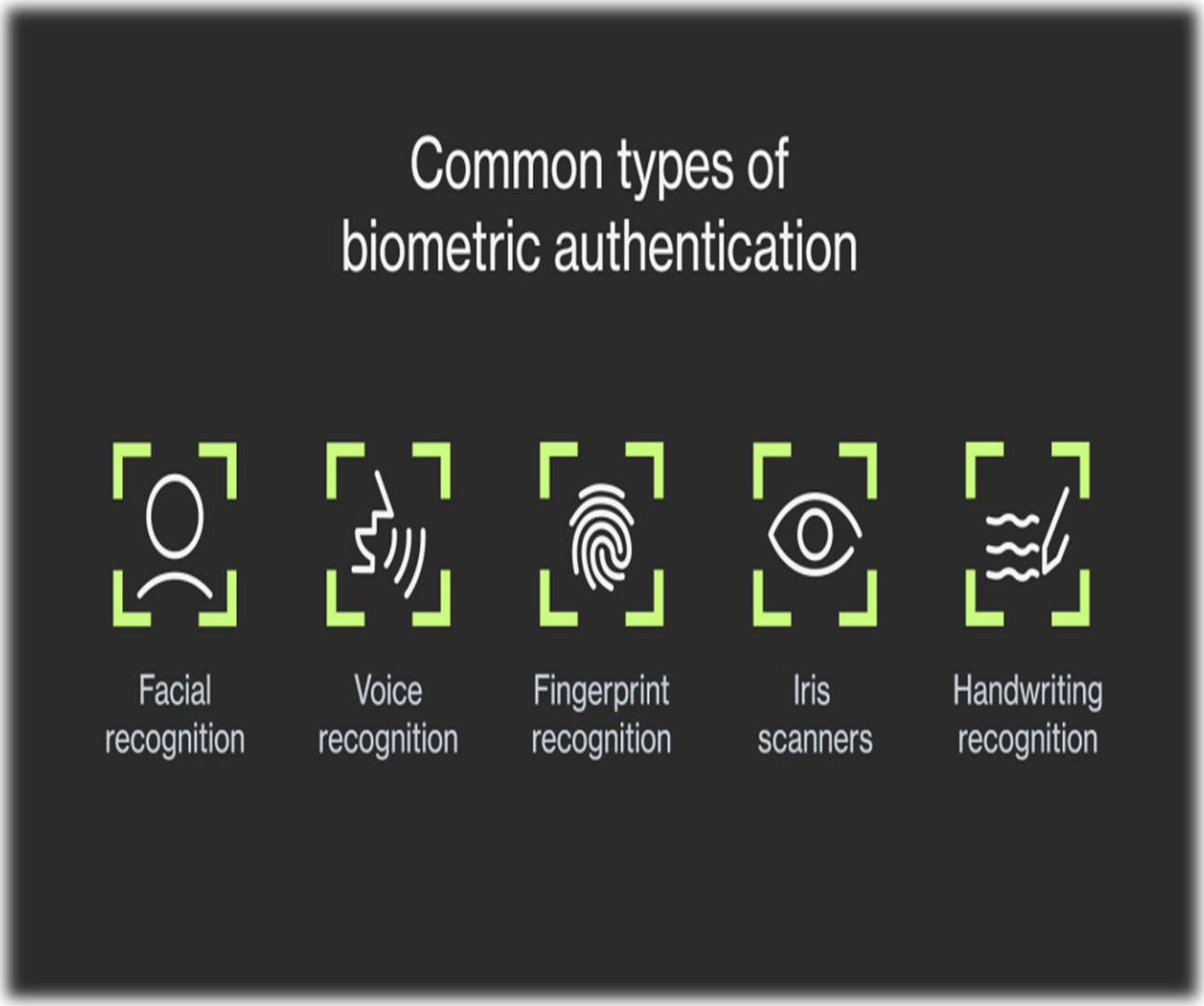
- The method used to commit the mobile fraud;
- Financial documents falsified by the perpetrator to conceal the mobile fraud;
- Bank account numbers changed, and corrupt payments effected;
- Details of suppliers over changing for goods in collusion with employees;
- Details of payments effected with no supporting documents;
- Details of personal purchases made on the business account.

7.3.2.1 Sub-Theme 2.2: Poor/ Inadequate Surveillance

Evidently, the surveillance of the ATMs or banks, particularly at biometric-based solution in combating mobile fraud is viewed by most narrative literature review from the following annual statistical reports: The SABRIC report on statistics recording incidences of 2018/2022 suggested a mediating factor to reduce and ultimately eliminate the scourge of biometric-based solution in combating mobile fraud at SABRIC. These answers corroborate perspective, which also noted that subpar service delivery was considered a significant contributing factor to mobile fraud. Because biometric authentication can provide extremely secure identity verification procedures, it is rapidly becoming an essential part of the banking sector. Aside from that, biometrics are also employed at ATMs, online banking, in-branch banking, and mobile banking (ACFE, 2022:np).

Biometrics are highly personal: However, opt-in biometrics do not expose consumers to surveillance. Given that biometric technology has only recently begun to enter the mainstream, consumers remain uncertain about what the technology includes and its potential applications (SABRIC, 2019:np). This uncertainty, understandably, results in various misconceptions and apprehensions. The truth is that opt-in biometrics provide the safest method for identifying mobile fraud while also safeguarding their information and identity from exploitation and they are considerably different from biometrics employed for surveillance purposes (AGSA, 2019:np). Remote biometric onboarding associates a person's biometric data, such as their facial features or fingerprint, with their account so that they, and exclusively they, can access the account in a safe and secure manner (Button *et al.,* 2017:70). This safeguards customers against fraud.

Figure 7.2: Biometric Payment Technology in the Banking Industry



Source: SABRIC Annual Report (2022:np)

7.3.2.3 Sub-Theme 2.3: Poor/ Lack of Training Support

Numerous literature sources, as well as annual statistical reports: SABRIC, ACFE, GSMA, ISPA, the INTERPOL, and the AGSA annual statistical reports from 2018/2022 mention that inadequate resources and training are contributory causes to problems that eventually affected the biometric-based solutions to combat mobile fraud. The accuracy and dependability of biometric systems is one of the primary issues, and such training is essential for tackling it. Biometric systems may fail to identify or validate people for a variety of reasons, such as user behaviour, ambient conditions, or sensor accuracy. For example, a fingerprint scanner may not work effectively if a finger is wounded, wet, or dirty. In the latter case, using undue force may incite criminals or those who are suspected of committing crimes to react, which may spark a surge in mobile fraud. The biometrics payment technology can be combined with biometric identification methods that utilise distinct eye structures with a high degree of security. Increasing the amount of data needed for precise authentication is the aim of improving the security of biometric systems. The narrative literature review (SABRIC, ACFE, GSMA, ISPA, INTERPOL) and AGSA annual statistical reports from 2018/2022) data analysis indicate that there was insufficient training, putting SABRIC at risk of facial recognition while dealing with mobile fraud. Emails, duty logs, calendars, scrapbooks, posts on Facebook, blogs, incident reports, reflections, and journals are a few examples (SABRIC, 2021:np).

7.3.2.4 Sub-Theme 2.4: Increasing legislation to prevent attacks

The narrative literature review from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, INTERPOL and the AGSA annual statistical reports from 2018/2022 of the biometric-based approach has the main aim to address mobile fraud at SABRIC. The prevalence of these SIM-related offenses extends beyond just financial crimes and SIM swap fraud (SABRIC, 2020:np). For the price of a few unregistered SIM cards at R5 a piece from a roadside seller, planning a murder becomes untraceable by police through RICA, making it virtually risk-free (GSMA,2020:np). In 2022, ICASA released preliminary regulations that would mandate mobile network operators to gather subscriber biometric data. ICASA indicated that these regulations would decrease occurrences of mobile number hijacking through fraudulent SIM swaps and number porting (ACFE, 2020:np). Nevertheless, this was met with reluctance from both consumers and organisations such as the Communications Risk Information Centre (COMRiC). Consumers were concerned that the collection of biometric data would invade their privacy, whereas COMRiC believed that relying solely on biometrics was too narrow in its approach and difficult to implement on a large scale (Button *et al.,* 2017:167).

7.3.2.5 Sub-Theme 2.5: The current state of SIM swap fraud

SABRIC (2022:np) reported a 9% decrease in mobile banking fraud committed in 2022, and that SIM swap incidents fell from 87% in 2021 to 76% (7,657) in 2022. Although this decrease is encouraging, there remain thousands of reported SIM swap fraud incidents every year. Cybercrime evolves and networks must be ready for increasingly advanced SIM swap attacks (ACFE, 2018:np). Their most effective defensive measure is to secure the identity of an individual associated with each SIM. The success of this method has been proven in countries such as Kenya, Namibia, Pakistan, and Russia, all of which have been implementing different levels of biometric SIM registration to discourage fraudsters (Button *et al.,* 2017:24).

It is also important to note that, in addition to Section 3.8 in Chapter 3, the data were analyses and presented in the context of widely held views in the literature in order to translate or transform the narrative literature review (annual statistical reports-2018/2022) into understandable conclusions with pertinent, useful, and significant real-world applications (Gray, 2019:11). Additionally, diagrammatic visualisations or graphical representations, have been utilised using figures, tables, and graphs to capture the key themes and the variables that are linked with them in line with the questions the researcher presented to the narrative literature review (annual statistical reports-2018/2022) (Vithal &Jansen*, 2019*:117). Also noteworthy is that the majority and minority patterns of narrative literature review (annual statistical reports-2018/2022) have served as a model on which the interpretations and conclusions were established.

7.3.3 Theme 3: The Challenges Encountered by the Forensic Investigators in the Investigation of Mobile Fraud at SABRIC

Published reports, including the SABRIC, ACFE, GSMA, ISPA, INTERPOL, as well as the AGSA annual statistical reports from 2018/2022 pertain to the third theme. *What are the challenges encountered by the forensic investigators in the investigation of mobile fraud at SABRIC?* The challenges encountered by the forensic investigators are as follows:

- ***Human Error and Bias:*** Forensic analysis and interpretation of evidence can be subjected to human error, bias, and the pressure to produce results.
- ***Sample Contamination:*** The integrity of evidence can be compromised by contamination, which can lead to inaccurate results.
- ***Technological Advancements:*** The rapid pace of technological change requires forensic professionals to constantly adapt and learn new techniques and tools.

- ***Digital Evidence and Cybercrime:*** The rise of digital evidence and cybercrime presents new challenges in extracting, analysing, and preserving data from digital devices.
- ***Anti-Forensics Techniques:*** Criminals are increasingly using anti-forensics techniques to conceal their activities, making it harder for investigators to access and analyses data.
- ***Encryption and Data Security:*** The use of encryption and other security measures makes it difficult to access and analyses data, requiring specialised expertise and tools.
- ***Data Volume and Complexity:*** The sheer volume and complexity of digital data can make it challenging to identify relevant information.
- ***Chain of Custody:*** Any break in the chain of custody can compromise the evidence, making it difficult to determine if the image has been altered during the investigation process.
- ***Emerging Technologies:*** New technologies like cloud computing, blockchain, and the Internet of Things (IoT) present novel challenges.
- ***Insufficient Tools or Resources:*** Departments conducting investigations may lack the necessary tools or resources to handle the volume and complexity of evidence.
- ***Staff Shortages and Retention:*** Forensic laboratories may face backlogs and delays in processing evidence due to staff shortages and difficulties in recruiting and retaining qualified personnel.
- ***Lack of Funding:*** Lack of funding can lead to delays in upgrading and modernizing forensic capabilities.
- ***Lack of Police Training:*** Lack of police training regarding forensic investigation can lead to damaging physical evidence on crime scenes.

Emotional and Psychological Challenges:

- ***Distressing Scenes:*** Crime scene investigators often encounter distressing scenes, including violent crimes and accidents, which can lead to emotional desensitization, heightened sensitivity, anxiety, and stress.
- ***Burnout:*** The high-pressure environment and long hours can contribute to stress and burnout.
- ***Trauma:*** Exposure to highly distressing scenes and materials can lead to trauma and mental health issues.
- ***Isolation and Disconnect:*** Forensic laboratories can be physically isolated, leading to feelings of isolation and disconnect.

- ***Existential Despair:*** Some forensic investigators report feelings of existential despair and disillusionment.

Ethical and Legal Challenges:

- ***Privacy Concerns:*** Forensic investigations often involve accessing sensitive data, raising privacy concerns.
- ***Data Authenticity and Admissibility:*** Ensuring the authenticity and admissibility of digital evidence is crucial but can be difficult due to the ease with which digital evidence can be altered or manipulated.
- ***Jurisdictional Issues:*** Digital evidence does not respect physical borders, making it difficult to determine which jurisdiction has the authority to seize and analyses it.
- ***Evolving Technology:*** The rapid pace of technological advancement constantly pushes the boundaries of existing legal frameworks, making it difficult to keep up with new types of digital devices, cloud storage solutions, and encryption methods.
- ***Misuse of Evidence:*** The potential for misuse of evidence and bias in interpreting results raises ethical concerns.

According to the fraud triangle theory, the researcher discovered that three factors, namely, offender motive, opportunity, and rationalisation must all come together for a mobile fraud act to take place. The confluence of four factors is necessary for a mobile fraud act to take place, as per the fraud triangle theory. In contrast to the fraud triangle idea, these contain (i) offender motivation, (ii) opportunity, (iii) rationalisation, and (iv) individual capability. One sub-theme or category emerged from the above-cited main or global theme, namely:

- **Addressing kidnapping crime.**

Furthermore, 2 (two) other sub-categories emerged from the afore-mentioned subtheme, namely:

- **Avoiding/ Reducing socialising in taverns and night clubs.**

7.3.3.1 Sub-Theme 3.1: Addressing app kidnapping financial crime

According to AGSA (2022:np), in this instance, the goal may be to demand a ransom be paid by the victim's family and SABRIC. The financial sector in South Africa is grappling with effects of smartphone banking in the aftermath of a concerning increase in kidnappings (ACFE, 2022:np).

Experts caution that the very security measures intended to protect users may inadvertently prolong hostage situations as a result of the rise in digital transactions. A financial expert has noted that ironically, because digital wallets and other phone-based payment methods offer extra protection, their growing use may result in protracted hostage situations. The 3,641 kidnapping incidents were reported to SAPS stations between April and June of 2023 (ACFE, 2022:np).

Considering the narrative literature review from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, INTERPOL and the AGSA annual statistical reports from 2018/2022 mentioned more instances in the future where an abducted person lacks cash and a card due to the increasing use of these digital payment features. As more perpetrators become aware of app kidnapping, they likely modify their tactics to continue depriving victims by hijacking vehicles then commit mobile fraud by app kidnapping (Sekhu, 2023:np). In relation to effectively implementing biometric identity for mobile devices at SABRIC to safeguard consumers and businesses from SIM-centric offenses, two essential criteria must be fulfilled: scalability and accessibility. SIM swaps continue to be a significant issue, and networks have yet to secure consumer protection fully (SABRIC, 2022:np). By ensuring identity validation for all SIMs at the time of registration, substantial progress can be achieved in enhancing protection against SIM-related offences. Although there is safety risks associated with mobile banking apps in areas where kidnapping is common, using mobile payment systems such as Google Pay, Apple Pay, or Samsung Pay can offer a safe and practical substitute for traditional credit cards (ACFE, 2021:np).

The method of operation utilised by the hijackers involves employing vehicles to abduct victims effectively, who are subsequently compelled by the perpetrators to make transfers from their banking applications at gunpoint (SABRIC, 2021:np). Sekhu (2023:np) stated in an interview on Kaya FM's 959 Breakfast show, that a crime expert pointed out that sometimes, the car is not even stolen by the hijackers. Instead, they merely utilise the vehicle to kidnap their victims, vanishing with both the victims and the vehicle (Sekhu, 2023:np). There is not much that can be accomplished when an individual is coerced into accessing his/her own profile on his/her phone through an app kidnapping. It is similar to when an individual uses his/her own card and pin to compel victims to withdraw cash from an ATM. In present times, the majority of vehicle crime incidents in South Africa are still hijackings, even though criminal syndicates use a variety of clever new tactics (ACFE, 2022:np). Based on the latest crime statistics, South Africa faces an average of approximately 60 car hijackings each day. According to the Tracker Vehicle Crime Index, theft constitutes 45% of vehicle crimes, while hijackings represent 55% (Sekhu, 2023:np).

Figure 7.3: Grayscale Photo



Source: Sekhu (2023:np)

A concerning trend in crime has surfaced in South Africa: the kidnapping of victims who are subsequently forced, often under the threat of violence, to make illicit transfers from their banking applications (Sekhu, 2023:np). Experts have observed an increase in the number of cases in which criminal syndicates target victims including business owners. The victims are made to complete a variety of acts against their will, including paying into foreign bank accounts, making online purchases, and withdrawing cash from ATMs. Traditional security mechanisms like pins, biometric verification, and facial recognition become useless as a result of the thieves preying on the victims' feelings of fear and intimidation (Sekhu, 2023:np).

A crime expert detailed his observations on this crime, on Kaya FM's 959 Breakfast show 959 Br. A concerning new criminal trend has surfaced in South Africa: victims get abducted and forced to transfer money from their banking apps, frequently under threat of violence. This often results in the victims losing all of their savings or entirely looting their other accounts. A crime expert spoke with a radio presenter and provided some perspective on this kind of crime. The pair discussed options available to customers in this circumstance. Since criminals use a variety of strategies to avoid discovery, the 'banking app kidnappings', as reported by TechCentral, (Staff Reporter, 2023:np) indicate that money is sometimes transferred outside South Africa, which makes tracking it almost impossible. Because the offenders frequently relocate, it is challenging for the authorities to capture them (Staff Reporter, 2023:np; SABRIC, 2023:np). This escalation in criminal activities has prompted financial institutions and security experts across South Africa's leading banks to alert the public about the risks and advise on preventive measures. Victims are left in a helpless situation during these incidents, leading some individuals to consider deleting their banking apps from their devices. However, this drastic measure complicates day-to-day transactions and financial management (Staff Reporter, 2023:np).

Some experts advise taking a middle-ground stance, in which people move the majority of their money to accounts with longer notice periods and only retain a small amount in their transactional accounts. Although this tactic helps victims lessen possible losses, it is not infallible (ACFE, 2022:np). High-risk people are frequently singled out, including kids, single people, company owners, people with large incomes, and immigrants to South Africa. Victims who are more likely to have complex account profiles and sizable balances are targeted by criminals because they present profitable opportunities (SABRIC, 2022:np). It is still difficult to identify and halt these shakedowns in process, even with heightened awareness.

Crime related to banking has been observed by the SABRIC (2022:np). Instances of banking app fraud have surged by 36%, showing a shift in criminal tactics, while other mobile banking crimes have dropped. Since they are less successful, once-popular strategies like SIM swaps are being abandoned by criminals. Because of this, kidnappings using banking apps occur on a regular basis, which calls for increased awareness and preventative actions to protect people from being victims of these crimes. In these terrible circumstances, victims are encouraged to put their safety first, comply with requests made by the kidnappers, work with them, maintain composure, memorise facts for future identification, avoid agitating them, and seek out assistance from banks and authorities after the ordeal is over.

7.3.3.2 Sub-Category 3.2: To trace the perpetrators app kidnapping crime of mobile fraud at SABRIC

Investigations into abduction-related complaints filed with the New Fund Offer (NFO) have revealed that, following their kidnapping and detention, criminals threaten and use violence to coerce banking customers into disclosing their online banking and banking app passwords (Button *et al.,* 2017:67). Banks' implementation of many security layers on their online platforms may be one reason fraudsters are resorting to this new method of operation. These steps are making it harder and harder for scammers to get private banking information from banking clients. After kidnapping and detaining the victim, criminals use threats of violence (duress) to coerce the victim into disclosing their online banking and banking app passwords.

7.3.4 Theme 4: The Best Practices to Combat Mobile Fraud at SABRIC

The ***fourth*** theme emerged from the narrative literature review from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, INTERPOL and the AGSA annual statistical reports from 2018/2022 statements in respect of the question: *How can society play a role in curbing and identifying best practices to combat mobile fraud at SABRIC?*

The aforementioned major or global subject gave rise to two sub-themes or categories regarding society's role in lowering the high percentage of mobile fraud in the South African banking sector. This position involves:

- Refraining from perceived hatred and jealousy; and
- Restoring trust between banking employees and the community.

7.3.4.1 Sub-Theme 4.1: Refraining from perceived hatred and resentment

The SABRIC's consumers ongoing hostility and victimisation due to mobile fraud were found to be the root reasons of the fraud (Bruce, 2022:15). As a result of their financial crimes and deceiving SABRIC's consumers, fraudsters have occasionally been perceived as sustaining financial fraud because of their actions and attitudes. The following narrative literature review (SABRIC annual statistical reports, ACFE annual statistical reports, GSMA, ISPA and the AGSA reports from 2018/2022) remarks suggest that bank clients are cheated due to jealousy from the community or private advisors they assist and live with.

The narrative literature review (annual statistical reports-2018/2022) suggests that the SABRIC's customers are scammed by fraudsters of mobile fraud by using SIM swap and app kidnappings. Based on published data and trends, predictive analytics uses statistical models and machine learning to predict the probability of fraudulent events. Among the techniques we can employ to identify fraud are neural networks, decision trees, and logistic regression (Bruce, 2022:16).

7.3.4.2 Sub-Theme 4.2: To effectively combat mobile fraud at SABRIC

SABRIC ought to embrace the subsequent best practices and remain aware of new trends. Keeping an eye on fraud patterns and adjusting detection systems to new threats is essential. Frequent updates and improvements by SABRIC (2020:np) to models and rules can assist in preserving the efficiency of fraud detection systems. Employing strong multi-factor authentication methods, including biometrics or one-time passwords, can greatly improve account security and lessen the chances of account takeover fraud (ACFE, 2021:np). New technologies, including blockchain and federated learning, show potential for boosting mobile fraud detection abilities. Blockchain can offer secure and clear transaction records, whereas federated learning allows for joint model training without sacrificing data privacy (SBARIC, 2022:np).

7.4 SUMMARY

This chapter presented the secondary data as non-empirical approach from the narrative literature review using annual statistical reports-2018/2022 regarding the prevalence and prevalence of mobile fraud at SABRIC. Also presented are factors that contribute to mobile fraud at SABRIC, challenges encountered by the forensic investigators in the investigation of mobile fraud at SABRIC, as well as the best practices to combat mobile fraud at SABRIC. The chapter include information on the demographic profiles of the narrative literature review from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, INTERPOL and the AGSA annual statistical reports from 2018/2022), as well as the four created themes and the sub-themes or categories that went along with them.

These four crucial themes, taken together, addressed the reasons behind the biometric-based approach used by the SABRIC to combat mobile fraud. Notwithstanding the difficulties that forensic investigators and banking subject matter experts encounter, the data suggest that there may be a window of opportunity for regulating investigation training programmes and strengthening the bonds between these professionals and the communities they serve in the South African banking sector. A summary of the primary and secondary research findings is given in the upcoming chapter.

CHAPTER EIGHT

SUMMARY, RECOMMENDATIONS AND CONCLUSION

8.1 INTRODUCTION

This chapter presented a summary of all the chapters, recommendations and conclusions based on the cited published literature as well as from: SABRIC. ACFE, GSMA, ISPA, INTERPOL and the AGSA annual statistical reports from 2018/2022. Furthermore, limitations of the study are sketched and the need for further research is stated.

8.2 SUMMARY

Chapter one presented a general orientation of the study, the dynamics of the communication industry which changed with the introduction of mobile telephones and the subsequent upgrades of mobile phones to provide financial services. This brought financial services closer to the general public by utilising the local merchant infrastructure already in place. This study investigated biometric-based strategies to prevent mobile fraud in the banking sector in SABRIC. The main goal aims to determine the type and scope of mobile fraud at SABRIC and to pinpoint the causes of mobile fraud at SABRIC, an increasing proportion of fraud instances go mostly unreported by the police, due to capacity constraints, posing a serious dilemma. It turns out that fraudsters in so-called general fraud cases have a relatively low conviction rate. These put forensic investigators' investigative abilities to the test, which have devastating results because it makes it harder to provide high-quality services.

Chapter two presented the research methodology, design and data collection, as well as the data analysis strategies that were followed in this study. The study location is indicated, and the following aspects are considered: the non-empirical perspective that the researcher believes in, methods used to ensure trustworthiness, as well as the ethical considerations, since it is important that the researcher followed the correct way of conducting research. It is very important to consider ethics in research.

Chapter three presented the prevalence of mobile fraud at SABRIC and the scope on the prevalence and extent of mobile fraud at SABRIC, and how to combat mobile fraud, particularly at the South Africa Banking Risk Information Centre. This is followed by a discussion to give effect to an overview of mobile fraud at SABRIC. This chapter provided an exploration of an overview of mobile fraud at SABRIC**.**

Chapter four discussed factors that contribute to mobile fraud at SABRIC as well as the contribution to mobile fraud, especially when it comes to the risk of fraud that causes mobile fraud at banking sectors (Nedbank, FNB, ABSA, STD and Capitec), among others. Fraud not only results in financial loss to customers, but it also affects the SABRIC service to the customers.

Chapter five presented the challenges encountered by forensic investigators when investigating mobile fraud in SABI. There are efforts carried out by the government, including strategies to mitigate cybercrime such as the establishment of SABRIC. It is encumbered with the responsibility of providing the SABI with the necessary information related to crime, risk management, to promote inter-bank synergy aimed at reducing the risk of bank and organised related crimes. Mobile fraud remains a major concern at SABRIC and in any sector that involves managing finances. Although endowed with positive innovation, new SABRIC (Nedbank, FNB, ABSA, STD and Capitec) channels and solutions may also open new avenues for fraudulent activities to take place and new vulnerabilities that can be exposed. Players across the ecosystem need to work together and continually improve security measures to keep bad actors at bay and protect the funds and data of the end users.

Chapter six presented the best practices in combating mobile fraud at SABI as benchmarked from other countries.

Chapter seven discussed the research presentation and interpretation of the research findings. Conversely, the chapter presented the actual non-empirical (practical or secondary) data or statements derived from the annual statistical reports-2018/2022 to the questions posed by the researcher during data collection sessions. In that regard, the criticality of the present chapter is underpinned by the prevalence to which it serves as the most pivotal reference point for the much-needed practical evidence of the study in relation to both the research problem and aim of the study.

Chapter eight elucidated the recommendations that were established based on the presented findings of the study and followed by the conclusion. The interpretations are carried out to address the investigative challenges and factors that are contributing to the failure of biometric-based solution in combating mobile fraud at SABRIC. The recommendations are made to strengthen the investigative process for exploring of biometric-based solution in combating mobile fraud at SABRIC. Furthermore, the Researcher developed a conceptual model in combating mobile fraud at SABRIC.

8.3 RECOMMENDATIONS

It is recommended that SABRIC must adopt new innovative and secured mechanisms of financial dealings to enhance innovation, security and flexibility to combat mobile fraud. Also, the institution should provide forensic investigators and banking subject matter specialists with regular opportunities for more regular and more rigorous in-service training to acquire knowledge and skills. Such training should entail the following, as posited by the ACFE (2022:np):

- SABI fraud tactics become increasingly sophisticated, as it is continuously seeking innovative solutions to verify users securely, protect sensitive information, safeguard their customers, and prevent fraud. Biometric verification is emerging as one of the most powerful tools in this struggle to keep abreast. Gaining rapid traction, this biometric technology provides a secure and efficient way to verify and authenticate users and protect systems.
- SABRIC is adopting biometric solutions to strengthen security, protect sensitive data, and enhance user experiences, making it a cornerstone of modern fraud prevention strategies. This thesis explored the growing impact of biometric verification in fortifying security and combating mobile fraud.
- De-escalation strategies involving the use of biometric technology and precautionary measures when responding to active crime scams should be actively sought and implemented.
- Inculcation of self-control and self-discipline for dignified behaviour that does not bring discredit to themselves and their organisation on, and off duty, and to also be discreet in their social behaviour and public appearances;
- Initiate processes for amending the constitution to include implementation of harsher sentences, such as life imprisonment for mobile fraud to deter reoccurrences;
- Review internal policies and procedures to ensure the implementation of proper safety measures and procedures that will increase the safety of the forensic investigators and banking subject matter specialists;
- Engage members of the community for restoration of trust and confidence among all the relevant stakeholders by hosting public awareness campaigns and educational road shows through social media, radio and television to eliminate any hostility or any enmity between communities, the forensic investigators and banking subject matter specialists.

8.3.1 Common Uses of Biometric Verification

Mobile device authentication: Mobile devices such as smartphones and tablets commonly use biometric verification methods like fingerprint recognition and facial recognition to authenticate users. This enables quick and secure access to the device, apps, and sensitive information without the need for passwords or PINs. Biometrics provide a higher level of security and convenience, reducing the likelihood of unauthorised access.

Banking and financial services: Biometric verification plays a crucial role in the banking and financial sectors, helping protect the users' accounts and transactions. Many banks use authentication for online banking, ATMs, and mobile banking apps, relying on fingerprint, facial, or voice recognition to verify the identity of customers. This not only enhances security but also prevents fraud and ensures that customers have a seamless experience when accessing their accounts.

Healthcare access and security: In healthcare, biometric verification is used to protect patient data and ensure that only authorised personnel can access sensitive medical records. Healthcare providers are increasingly adopting fingerprint and iris recognition systems for secure patient identification, enabling faster and more accurate access to medical history. This reduces the risk of identity theft and improves the overall efficiency of healthcare systems.

Travel and airport security: Biometric systems have revolutionised the travel industry, especially at airports, where they are used for passport control, check-in processes, and security screenings. Facial recognition and fingerprint scanning help speed up these procedures, reducing waiting times and enhancing passenger experience. Biometrics also improve security by verifying the identity of travellers, ensuring that only authorised individuals are allowed to board flights or access secure areas.

Workplace access control: Biometric verification is widely used in workplaces for access control to restrict areas and to monitor attendance. Fingerprint, facial, and palm vein recognition systems allow organisations to manage employee access to sensitive areas securely while ensuring that only authorised personnel are granted entry. This minimises the risk of security breaches and enhances workplace safety.

Government and national Security: Governments use biometric verification to ensure secure identification for a range of services, including issuing passports, national ID cards, and voter registrations. Biometric data such as fingerprints and facial recognition are used in national security systems to detect and prevent identity fraud, as well as to enhance border control procedures. This technology helps streamline administrative processes and strengthens national security efforts.

E-commerce and Online Services: As the demand for online services continues to rise, e-commerce platforms are increasingly adopting biometric authentication to enhance the security of online transactions. By using fingerprint or facial recognition, these platforms can verify the identity of users and ensure that transactions are authorised. This reduces the risk of online fraud and builds trust with customers, offering a secure and convenient alternative to traditional password-based authentication.

Biometric verification is transforming how industries approach security, providing more accurate, efficient, and user-friendly solutions to identity management. As its applications continue to grow, the technology is setting a new standard in safeguarding sensitive information and enhancing user experiences across various sectors.

The reduction and prevention of mobile fraud is an indispensable requirement for both the maintenance of law and order, as well as restoration of the public's trust in the capacity of the forensic investigators and banking subject matter specialists to protect them, their lives and their property. Both are not in the list. As such, the establishment of more effective policies and regulations could minimise the irregularities that might have been identified in the present police training strategies (ACFE, 2022:np). Policy modifications, training improvements, and other measures could alleviate the prevalence of the forensic investigators and banking subject matter specialists by evaluating the data concerning the magnitude of clients who have been victims of mobile fraud.

Furthermore, improvement of public awareness in the investigation of mobile fraudster organisational structure is helpful insofar as conscientious citizens to become more aware of the biometric-based solution in combating mobile fraud at SABRIC (ACFE, 2022:np). Pressure emanating from the public might result from increased public awareness to the uncontrolled and unresolved problem emanating from tensions within the society and loss of trust in the forensic investigators and banking subject matter specialists.

- ***There are risks in most situations:*** Risk management is an important element of SABRIC to review risk status and developmental approaches relating to mobile fraud.

- ***Development of Smart Tools and Processes:*** Smart tools and processes are important in the management of fraud. Most fraud, especially those of a larger scale/magnitude, can be detected and limited through effective data analytics. Many deployments have failed to employ real time, efficient and reliable analytics in SABRIC data.

In order to remedy this weakness, deployments may be forced to develop new and better platforms or create interfaces that will enable generation of proper data for SABI (ACFE, 2022:np).

- ***Research:*** There is very limited research of fraud in mobile financial services. This is largely because mobile financial services are fairly new globally, with a limited range of successful deployments. Research would involve working closely with these deployments to understand the risks of fraud. In many cases, deployments will be very sensitive about the type of organisation they work with in order to protect their sensitive data (ACFE, 2022:np). They are therefore more likely to work with independent reputable organisations that are unlikely to compromise on their data. Donors and consultants can play a key role in identifying neutral parties to carry out this research which in the long term benefits the entire industry. Research will help the market understand the core reasons for fraud, frequency of occurrence, patterns, responsible parties and the effectiveness of various interventions carried out to curtail frauds.

- ***Client Protection Reviews:*** Client protection measures are those measures that are in place to protect consumers and other users of mobile financial services and therefore the industry itself from unfair practices. A formal review of banking sectors' ability to optimise client protection and thus reduce operational, fraud and reputation risk can be carried out through a series of agent, consumer, staff and senior management interviews (and use of other PRA tools). Donors should support these client protection reviews to protect the nascent SABI from shocks as recently seen in the micro-finance industry (ACFE, 2022:np).

The use of industry lobby groups, especially association of mobile fraud providers should be encouraged to set standards that protect consumers. Standards set by an industry association can work to ensure that all providers roll out fair products and take measures that will maintain credibility of services of the industry. Such associations may even work towards uniformity of cross network standards and peer reviews to check compliance to standards agreed collectively (ACFE, 2022:np). Such associations may lobby governments on implementation of certain policy actions like counterfeit awareness campaigns to reduce fraud.

Obtaining evidence - The reliability of the evidence gathered determines the usefulness of a fraud examination. Fraud examiners must be aware of the right and legal ways to gather documentary evidence

and witness statements since most forms of fraud evidence are in the form of papers or statements made by witnesses (Button *et al.,* 2017:129).

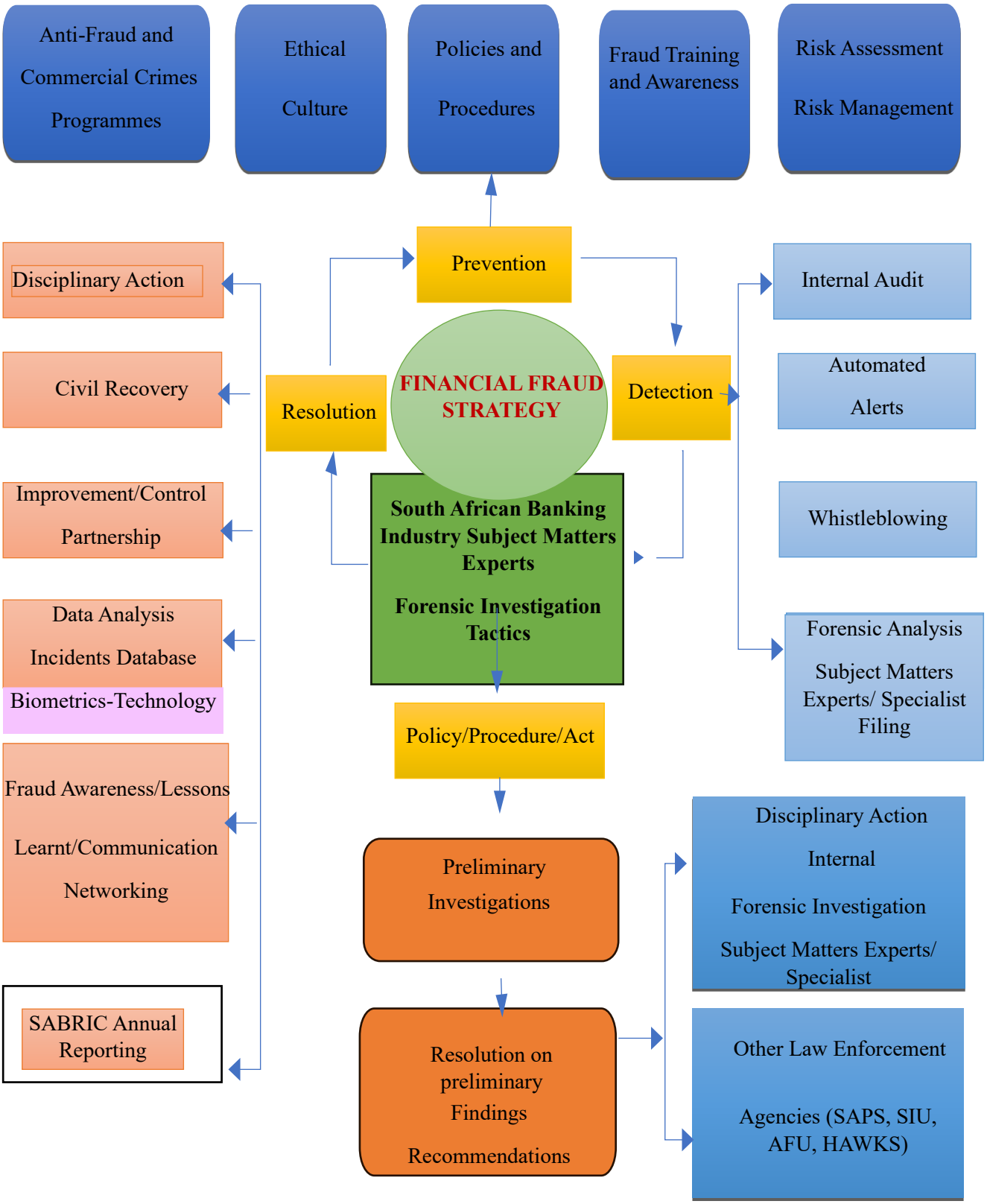
Reporting - The fraud examiner must inform the designated persons of the conclusions when evidence has been gathered, examined, and drawn (e.g., management, the board, or the audit committee). A fraud examination report is a narrative of the precise actions, conclusions, and, if necessary, recommendations of the fraud examiner. The management must have these messages to decide the best course of action. There are several methods to share an examination's findings.

The best way to convey information varies depending on the facts at hand, although most reports are delivered orally or in writing. When communicating the results of a fraud examination, the fraud examiner is responsible for providing clear, accurate and unbiased reports reflecting the fraud examination results (Button *et al.,* 2017:136). This need arises from the possibility that these results might end up being read or used by various groups of people, such as organisations insiders, PwC, KPMG, Deloitte and other law enforcement deals with mobile fraud.

Testifying to findings - Fraud investigators are frequently asked to testify and present their findings at a deposition, trial, or other legal action. Fraud examiners must tell the truth while testifying. They should also communicate clearly and succinctly (Button *et al.,* 2017:142).

Assisting in fraud detection and prevention - The management or other relevant authorities are in charge of preventing fraud, not the fraud examiners (Button *et al.,* 2017:86). However, fraud examiners are required to seek out and suggest suitable laws and regulations to stop fraud actively, particularly when their investigations reveal problems with fraud controls. Solely on the basis of their education, experience and training, CFEs are uniquely qualified to assist organisations in preventing and detecting fraud.

Figure 8.1: Mokopane Fraud Model-24



Source: Researcher illustration (2024)

The structure illustrated in figure 8.1 provides guidelines for a Mokopane Fraud Model-24. Law Enforcement Agencies and SABRIC can be flexible in developing a model suitable for their circumstances. The guidelines are more about understanding the principles and are not blueprints. The structure named as Mokopane Fraud Model-24 aims to assist the Law Enforcement Agencies and SABRIC as well as subject matter specialists in mobile fraud. MFIP provides all structures related to law enforcement and risk management. Mokopane Fraud Model-24 recommends that SABRIC should work together with the following law enforcement agencies: - SAPS, HAWKS, Special Investigation Unit, Border Management Authority, Traffic Officers and service providers (i.e., MTN, Vodacom, C-Cell and Telkom) to combat mobile fraud and app kidnapping relating to the transaction of money (SABRIC annual reports-2018/2022).

8.3.2 Mokopane Fraud Model-24: Financial Fraud Strategy

The **"Mokopane Fraud Model-24"** is most likely a model designed to prevent and detect financial fraud. This model focuses on financial fraud prevention and detection strategies, potentially incorporating machine learning and other techniques.

Key Elements of a Fraud Model:

- **Risk Assessment**

It should identify areas within the organisation that are vulnerable to fraud (e.g., procurement processes, financial transactions, etc.).

- ***Fraud Prevention Measures-*** Implementing controls to deter fraud, such as segregation of duties, authorisation controls, and internal audits.
- ***Fraud Detection Mechanisms-*** Establishing systems and processes to identify suspicious activities that may indicate fraud.
- ***Data Analysis-*** Analysing financial data for patterns and anomalies that could indicate fraudulent transactions.
- **Behavioural Analysis-** Monitoring user behaviour and patterns to detect unusual activity.
- **Machine Learning-** Using algorithms to identify fraud patterns and predict potential fraud cases.

Fraud Response Plan:

Developing procedures for investigating potential fraud cases and taking corrective actions.

- ***Training and Awareness*- Educating employees about fraud risks and the organisation's fraud prevention policies.**
    - ***Legal and Ethical Framework*:** Outlining the legal and ethical guidelines for dealing with fraud cases.

Mokopane Fraud Model-24 fraud prevention plan includes:

- ***Risk identification and assessment-*** Identifying vulnerabilities in their operations.
- ***Responsibility for fraud risk-*** Assigning responsibility for fraud risk management.
- ***Response plan-*** Developing procedures to address fraud cases.
- ***Legal framework-*** Outlining relevant laws and regulations.

In the context of the "Mokopane Fraud Model-24", it is likely that a similar approach would be taken, with a focus on the specific financial fraud risks within the organisation. This model would aim to integrate various techniques and strategies to prevent, detect, and respond to financial fraud effectively:

- Determine the fraud risk management activities to be performed considering the fraud risk profile and related costs versus the benefits.
- Determine the resourcing requirement (this element describes the capacity and competence of personnel and the strategy to address capacity gaps. It also addresses the technology and funding requirements needed to implement the fraud risk management strategy).
- Determine the sequence of activities and the target implementation dates, assign ownership for and communicate fraud risk management activities, agree on frequency and format of reporting and obtain consensus on the frequency, content and responsibility for reporting.
- The size of SABRIC and the prevalence of fraud and corruption can be used to decide whether to have a separate oversight committee for fraud risk management and to use the risk management committee as an oversight body.
- The fraud prevention strategy and implementation plan should ideally be developed together to ensure connectivity and continuity. Both documents should be approved by the accounting officer/authority and reviewed annually.

8.4 LIMITATIONS OF THE STUDY

Normally, limitations of a study and challenges experienced by a researcher are not necessarily an indication of the study's weakness or failure to achieve its stated objectives (Korstjens & Moser, 2018:122). For this study, cited literature sources included SABRIC annual statistical reports, ACFE annual statistical reports, GSMA, ISPA and the AGSA reports from 2018/2022 for statistical data collection of the literature review of the study. Other literature sources were the annual statistical reports-2018/2022. This study did not involve human participants, rather it involved citing literature studies (annual statistical reports-2018/2022) and other internal data relating to the area of research from 2018/2022. The population and sampling are expressed under the narrative literature review (annual statistical reports-2018/2022) and other internet data relating to the area of research from 2018 to 2022.

8.4.1 Lack of Data

There were constraints of accessing the information from various areas because the confidential prevalence of the required information needed to be authorised. There were limited data on the circumstances surrounding each incident. It was difficult for the researcher to draw meaningful data as the causes of mobile fraud of each victim were not provided. In addition, the lack of adequate prior studies on the topic of mobile fraud presented a constraint to the researcher's accurate determination of the causes of mobile fraud. As such, the researcher had to compare each incident of a mobile fraud from other sources in order to acquire meaningful data.

8.4.2 Narrative literature review (Annual Statistical Reports-2018/2022)

Much data was sourced from literature sources particularly that on annual statistical reports: SABRIC, ACFE, GSMA, ISPA, the INTERPOL and the AGSA annual statistical reports from 2018/2022 which established the importance of data analysis. Furthermore, regarding the narrative literature review (Annual Statistical Reports-2018/2022) that carries the victim's database of mobile fraud, the limitations are due to the reluctance of literature review (narrative literature review- annual statistical reports-2018/2022) about sensitive issues and the lack of official data on the analysis conducted by the SABRIC for the period 2018/2022.

8.4.3 Time Constraints

The literature review using the following sources (SABRIC, ACFE, GSMA, ISPA, the INTERPOL and the AGSA annual statistical reports from 2018/2022) unpacking from the SABRIC after conducting non-empirical research (secondary data collection) as narrative literature review.

8.4.4 Generalisation

The study findings were not generalisable to the forensic investigators or banking subject matter experts of SABRIC or other countries experiencing similar problems associated with mobile fraud, with various social, political, or financial systems. In this regard, caution is required while applying the study conclusions to different settings. The generalisability is not necessarily the main object in qualitative research studies.

8.5 RECOMMENDATIONS FOR FURTHER RESEARCH

Further research in any field of study or discipline is a perennial and indispensable requirement, given the fluidity of the human condition and its associated dynamics (Flick, 2020:16; Vithal & Jansen, 2019:46). It is in that regard that the recommendations for further research are intended mostly for improvement and development in those areas of the research field where the researcher has determined the need for such.

The aim of this study was to explore the prevalence, causes, and consequences of the biometric-based solutions in combating mobile fraud at SABRIC. In this regard, further research is recommended for the magnitude of combating mobile fraud at SABRIC jurisdictions in the entire country (ACFE, 2022:np). Such studies should also focus on the proportion of the biometric-based solution in combating mobile fraud at SABRIC.

In addition, these studies should also investigate or explore the prevalence of training techniques and approaches by the forensic investigators and banking subject matter specialists' structures to detect the weaknesses, compare and integrate the strengths, and apply a uniform approach since both SABRIC and the various forensic investigators and banking subject matter expect are essentially involved in the maintenance of various aspects of law and order (ACFE, 2022:np).

8.6 CONCLUSIONS

This chapter presented recommendations and conclusions. In this study, it is concluded that digital evidence is the most reliable form of evidence in mobile fraud when compared with other types of biometric-based solutions in combating mobile fraud that are subject to manipulation. Both primary or secondary evidence and available literature reveal that several factors including lack of experience and qualifications in crime scene management contribute to some prevalence to evidence contamination (annual statistical reports-2018/2022). The findings of this study also reveal that there are set procedures that should be followed when managing a mobile fraud and collecting digital evidence and a failure to adhere to these procedures can lead to evidence contamination. Overall, the insights that emerged from the secondary data were confirmed by the available literature, which meant that the set objectives of this study at the beginning were achieved.

Based on the findings of this study and its attendant recommendations, the following conclusions were drawn:

- It is essential to involve and engage the community to build trust between the banks and the public in order to combat mobile fraud.
- It is crucial to work towards improving training, adequate resources, and better management style and to keep up with technology as SABI experts are in the Fourth Industrial Revolution.
- It is crucial to review the existing policies and guidelines to ensure that they are under nationally prescribed best practices, which will help to improve biometric-based solutions in combating mobile fraud.

Furthermore, SABRIC ensures that only authenticated individuals are granted access, which markedly lowers risks such as identity theft and fraudulent account creation. It is advised that by utilising infrared light, the technology delineates the vein pattern and establishes a template for comparison. This technique is extremely secure due to the fact that vein patterns are hard to duplicate and maintain consistency over a person's lifespan. Some financial institutions and healthcare organisations implement vein recognition, adding an extra layer of security for identity confirmation. Furthermore, they ought to evaluate the effectiveness of their existing controls regularly in relation to newly arising fraud threats. Each of these biometric identity verification techniques is crucial in bolstering security, minimising fraud, and enhancing user experience. As technology progresses, these techniques are becoming more prevalent in both personal and professional settings, assisting organisations in better safeguarding sensitive data and facilitating smooth authentication processes.

LIST OF REFERENCES

ACFE. 2018. Occupational fraud. A report to the nations. Available at: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2018/2018-report-to-the-nations.pdf (Accessed on: 16 January 2023).

ACFE. 2019. Occupational fraud. A report to the nations. Available at: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2019/2019-report-to-the-nations.pdf (Accessed on: 16 January 2023).

ACFE. 2020. Fraud 101: What is Fraud? Available at: https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud (Accessed on: 16 January 2023).

ACFE. 2021. Fraud 101: What is Fraud? Available at: https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud (Accessed on: 16 January 2023).

ACFE. 2022. Occupational fraud. A report to the nations. Available at: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2022/2022-report-to-the-nations.pdf (Accessed on: 16 January 2023).

Adekanya, F. 1986. Fraud in banking transactions. 1(6), pp. 34-67.

Afonin, O. & Katalov, V. 2016. *Mobile fraud – advanced investigative strategies*. Birmingham: Packt Publishing

AGSA. 2018. Annual report for fraud. Available at: https://www.agsa.co.za/Reporting/AnnualReport.aspx (Accessed on 11 March 2023).

AGSA. 2019. Annual report for fraud. Available at: https://www.agsa.co.za/Reporting/AnnualReport.aspx (Accessed on 11 March 2023).

AGSA. 2021. Annual report for fraud. Available at: https://www.agsa.co.za/Reporting/AnnualReport.aspx (Accessed on 11 March 2023).

AGSA. 2022. Annual report for fraud. Available at: https://www.agsa.co.za/Reporting/AnnualReport.aspx (Accessed on 11 March 2023).

Albshaier, L., Almarri, S. & Hafizur Rahman, M.M. 2024. A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. *Computers*, 13(1), p. 27.

Al-Ghamdi, B.A.M.A. 2023. Selection of a Trustworthy Technique for Fraud Prevention in the Digital Banking Sector. *International Journal of Advanced Computer Science & Applications*, *14*(11).

Ambashtha, K.L. & Kumar, P. 2023. Online fraud. In: C.M. Gupta (ed). *Financial crimes: A guide to financial exploitation in a digital age* (pp. 97-108). Cham: Springer International Publishing.

Ambe, K.N. 2024. Analysis of the risk associated with bank crimes in Africa. *SSRN 4708322*.

Andrea, D. P., Olivier, C., Yann, B, Serge, W. & Gianluca, B. 2014. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, 41(1), pp. 4915–4928.

Annalise, K. 2022. E-mail can cause. Cybersecurity vulnerability in your organisations. *Servamus Community-Based Safety and Security Magazine,* 115(10), pp. 20-21.

Anney, B. 2014. Ensuring the Quality of the Finds of Qualitative Research: Looking at the Trustworthiness Criteria. *Journal of Emerging Trend in Educational Research and the Policy,* 5(2), pp. 272-281.

Ary, D., Cheser, L., Sorensen, C. K. & Walker, D. A. 2019. *Introduction to research in education* (10th edition). Boston: Cengage.

Ashbourn, J. 2014. *Biometrics: advanced identity verification: the complete guide*. Springer.

Babbie, E. & Mouton, J. 2021. *The practice of social research*. Cape Town: Oxford University Press.

Babbie, E. 2017. *Basics of Social Research* (7th ed.). Cengage Learning.

Babbie, E. 2021. *The practice of social research* (15th edition). Australia: Cengage Learning.

Bachman, R. K. & Schutt, J. 2015. *Fundamentals of Research in Criminology and Criminal Justice* (3rd edition). London: Sage.

Bair, J. 2017. *Seeking the truth from mobile evidence*. Massachusetts: Academic Press.

Barker, R. 2018. Knowledge management to prevent fraudulent e-banding transactions. *Communitas*, 23(1), 71–86.

Batra, V. S., Garg, D., Kothari, R., Krishnapuram, R., Negi, S., & Parija, G. R. 2013. *Detecting fraudulent mobile money transactions.* US8458090 B1.

Bertram, C. & Christiansen, I. 2014. *Understanding Research: An Introduction to Reading Research.* Van Schaik, Pretoria.

Bishop, D.Y. 2022. Fraud Risk Management to Detect and Prevent Employee Fraud in Small Rural Businesses. Doctoral Thesis. Virginia: Liberty University.

Boorman, J. and Ingves, S., 2019. Financial system abuse, financial crime and money laundering. *IMF Monetary and Exchange Affairs and Policy Development and Review Departments*.

Bougie, R. & Sekaran, U., 2016. *Research methods for business: A skill building* (7th edition). India: Wiley Publishers.

Brandl, S.G., 2017. *Criminal investigation*. Sage Publications.

Brody, R.G., Kern, S. & Ogunade, K., 2022. An insider's look at the rise of Nigerian 419 scams. *Journal of Financial Crime*, 29(1), pp. 202-214.

Brown, K., & Smith, J., 2022. The Role of Quantitative Finance in Financial Market Analysis and Decision-Making. *Financial Analysts Journal,* 78, 44-60.

Brungs, A., Winchester, D., Stephens, G. & Smith, S., 2018. The power of hermeneutic phenomenology in restoring the centrality of experiences in work-integrated learning. *International Journal of Work-Integrated Learning*, 19(3), pp. 261-71.

Bryman, A. 2012. *Social Research Methods.* Oxford: Oxford University Press.

Bryman, A. 2021. *Social research methods.* (6th ed). Cape Town: Oxford University Press.

Brytting, T., Minogue, R. & Morino, V. 2019. *The Anatomy of Fraud and Corruption: Organisational Causes and Remedies.* Britain: Gower Publishing Ltd.

Buckles, T. 2017. *Mobile fraud Scene Investigation: Criminalistics and the Law*. New York: Thomson Delmar Learning.

Burrell, D.N. 2023. *Transformational interventions for business, technology, and healthcare*. IGI Global.

Button, M. and Cross, C., 2017. *Cyber frauds, scams and their victims*. Routledge.

Casey, E. 2021. *Digital evidence and computer crime* (3rd ed). Massachusetts: Academic Publishing.

Castillo, E. 2009. *A Unified Statistical Methodology for Modeling Fatigue Damage*. Berlin: Springer.

Caulfield, T. & Steckler, S. 2014. "*The five faces of Mobile fraud, abuse, and noncompliance*", Contract Management, Vol. December, pp. 38–45.

Chandra, A. & Calderon, T. 2005. Challenges and constraints to the diffusion of biometrics in information systems. *Commun. ACM*, 48(12), pp. 101-106.

Chatain, P. L., Hernández-Coss, R., Borowik, K. & Zerzan, A. 2018. *Integrity in Mobile Phone Financial Service*s. World Bank Work. Pap.

Clark, T., Foster, L. & Bryman, A. 2019. *How to do your social research project or dissertation*. United Kingdom: Oxford University Press.

Coppolino, L., D'Antonio, S., Formicola, V., Massei, C. & Romano, L. 2015a. Use of the Dempster-Shafer Theory for Fraud Detection: The Mobile Money Transfer Case Study, in: *Intelligent Distributed Computing VIII*. Springer, pp. 465–474.

Coppolino, L., D'Antonio, S., Formicola, V., Massei, C. & Romano, L. 2015b. Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. *J. Ambient Intell. Humaniz. Comput*, 6 pp. 753 - 762.

Cressey, D. R. 1953. *Other people's money: a study in the social psychology of embezzlement*. Glencoe, IL: The Free Press.

Creswell, J. W. & Poth, C.N. 2018. *Qualitative inquiry & research design-choosing among five approaches* (4th edition). London: Sage Publications.

Creswell, J.W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (4th Edition). Thousand Oaks: Sage.

Creswell, J.W. 2020. *Research design* (6th edition). Thousand Oaks (CA): SAGE.

David, R. & Thomas, I.H. 2018. *Designing and planning your research project: Core skills for social and health research*. Chicago: Sage Publications.

Davis, J. S. & Pesch, H.L. 2013. Fraud dynamics and controls in organisations, *Accounting, Organisations and Society*, 38(6–7), pp. 469–483.

Dawson, S. 2015. *Internal control/anti-fraud program design for the small business: a guide for companies do not subject to the Sarbanes-Oxley Act*. John Wiley & Sons.

De Vos, A., Strydom, H., Fouche, C. & Delport, C. 2011. *Research at Grass Roots: For Social Sciences and Human Services Professions*. South Africa: Van Schaik Publishers, Pretoria.

Delamaire, L., Abdou, H. & Pointon, J. 2019. Credit card fraud and detection techniques: a review. *Banks and Bank Systems*, 4(2), pp. 57–68.

Denscombe, M. 2012. *Research Proposals-A practical guide*. McGraw- Hill House: Open University Press.

DePoy, E. & Gitlin, L.N. 2016. *Introduction to Research: Understanding and Applying Multiple Strategies* (5th Edition). USA: Elsevier

Douglas, J.E., Burgess, A.W., Burgess, A.G. & Ressler, R.K. 2013. *Crime classification manual. A standard system for investigating and classifying violent crimes.* Hoboken: John Wiley & Sons.

Dunham, K. 2008. *Mobile malware attacks and defense*. USA: Syngress.

Dzomira, S. 2014. Digital forensic technologies as fraud risk mitigation tools in the banking industry: evidence from Zimbabwe. *Risk Gov. Control Finance. Mark. Inst*, 4, 116.

Faundez-Zanuy, M. 2016. Biometric security technology. Aerospace and Electronic Systems Magazine, *IEEE*, 21(6), 15-26.

Ferguson, G. 2017. *Global corruption: law, theory and practice* (3rd edition). Victoria: University of Victoria.

Ferrari, R., 2015. Writing narrative style literature reviews. *Medical writing*, *24*(4), pp.230-235.

Fisman, R. & Miguel, E. 2017. Corruption, norms, and legal enforcement: evidence from diplomatic parking tickets. *Journal of Political Economy*, 115, pp. 1020-1048.

Flick, U. 2020. *Introducing Research methodology: A beginner guide to doing a research project*. London: SAGE.

Forte, D. 2013. Biometrics: Future Abuses. Computer Fraud & Security. *Computer Fraud and Security,* 2013(10), pp. 12-14.

Gehl, R. and Plecas, D., 2017. *Introduction to criminal investigation: Processes, practices and thinking*. Justice Institute of British Columbia.

Girard, J. E. 2021. *Criminalistics: Forensic Science and Mobile fraud*. Burlington: Jones and Bartlett.

Global System for Mobile Communications Association [GSMA]. 2022. Mobile money fraud typologies and mitigation strategies. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2022/03/GSMA-Fraud-Typologies-.pdf (Accessed on 11 March 2023).

Gray, D. E. 2014. *Doing research in the real world*. London: SAGE.

Gray, D. E. 2019. *Doing Research in the Real World* (5th edition). London: SAGE Publication.

Greenhalgh, T., Thorne, S. and Malterud, K., 2018. Time to challenge the spurious hierarchy of systematic over narrative reviews? *European journal of clinical investigation*, *48*(6), p.e12931.

Gruber, T. R. 1995. Toward principles for the design of ontologies used for knowledge sharing. *Int. J. Hum. -Computer. Stud*. 43, pp. 907–928.

Hayashi, F. 2012. Mobile payments: What's in it for consumers? *Economic Review-Federal Reserve Bank of Kansas City*, p. 35.

Hennink, M., Hutter, I. & Bailey, A. 2020. *Qualitative research methods* (2nd edition). Sage Publications.

Henriksen, R. 2007. Warriors in combat–what makes people actively fight in combat? *Journal of strategic studies*, 30(2), pp. 187-223.

INTERPOL. 2020. Interpol Warns of Financial Fraud Linked to COVID-19. Available at: http://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraudlinked-to-COVID-19 (Accessed on 10 July 2023).

INTERPOL. 2021. The two banks with the biggest increase in complaints in 2021. https://www.moonstone.co.za/the-two-banks-with-the-biggest-increase-in-complaints-in-2021/ (Accessed on 10 July 2023).

ISPA. 2020. Available at: Internet-Service-Providers-Association-ISPA-Submission-MDPMI-Provisional-Report-2022.pdf (Accessed on 07 April 2023).

ISPA. 2021. Available at: Internet-Service-Providers-Association-ISPA-Submission-MDPMI-Provisional-Report-20230407.pdf (Accessed on 07 April 2023).

ISPA. 2022. Available at: Internet-Service-Providers-Association-ISPA-Submission-MDPMI-Provisional-Report-2022pdf (Accessed on 07 April 2023).

Jain, A.K., Deb, D. and Engelsma, J.J., 2021. Biometrics: Trust but verify. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(3), pp.303-323.

James, S.H. & Nordby, J. 2018. *Forensic science. An introduction to Scientific and Investigative Techniques* (3rd edition). Boca Raton: CRC Press.

Jansen, J. and Leukfeldt, R. 2015, July. How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In *2015 workshop on socio-technical aspects in security and trust* (pp. 24-31). IEEE.

Khaldi, K. 2017. Quantitative, qualitative or mixed research: Which research paradigm to use. *Journal of Educational and Social Research*, 7(2), pp. 15-24.

KPMG. 2013. KPMG Malaysia Fraud, Bribery and Corruption Survey and Others. Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/fraud-survey-report.pdf (Accessed on 09 May 2022).

Kruse, C., 2015. *The social life of forensic evidence*. Univ of California Press.

Kumar, R. 2020. *Research methodology: A step-by-step guide for beginners* (6th ed.). USA: SAGE Publications Inc.

Kumar, R. 2021. *Research Methodology- a step-by-step guide for beginners* (7th ed.). London: SAGE Publications.

Labuschagne, G. 2015. Criminal Investigative Analysis: An Applied Perspective. In R.J. Zinn, & S.I,. Dintwe (Eds.). *Forensic Investigation: Legislative Principles and Investigative Practice*. Cape Town: Juta.

Laleh, N. & Azgomi, A. 2019. An overview of a hybrid fraud scoring and spike detection technique for fraud detection in streaming data. *Proceedings of the 3rd International Conference on Information Systems, Technology and Management.* Ghaziabad, India, 12–13 March, pp. 356–367.

Leavy, P. 2022. *Research design: Quantitative, qualitative, mixed methods, arts based, and community-based participatory research approaches*. New York: The Guilford Press.

Leedy, P. D. & Ormrod, J. E. 2016. *Practical Research: Planning and Design* (11th ed.). Upper Saddle River: Pearson Education. Inc.

Lokanan, M. E. 2015. Challenges to the fraud triangle: Questions on its usefulness. *Accounting Forum*, 39(3), pp. 201–224

Lopez-Rojas, E. A. & Axelsson, S. 2022. Multi agent-based simulation (mabs) of financial transactions for anti-money laundering (aml), in: *Nordic Conference on Secure IT Systems*. Blekinge Institute of Technology.

Luo, X. 2014. *Suspicious Transaction Detection for Anti-Money Laundering. Int. J. Secur*, 8(2), pp. 157-166.

Lusthaus, J. 2018. *Industry of anonymity: Inside the business of cybercrime*. USA: Harvard University Press.

Malady, L., Buckley, R.P. & Arner, D.W. 2014. Developing and Implementing AML/CFT Measures Using a Risk-Based Approach for New Payments Products and Services. *CIFR Pap*.

Marakalala, M. C. 2023. Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud. *ODA International Journal of Sustainable Development*, 16 (5), pp. 19-30.

Maree, J.G.K. 2017. Opinion Piece: Using Career Counselling to Address Work-Related Challenges by Promoting Career Resilience, Career Adaptability, and Employability. *South African Journal of Education*, 37(4).

Marohn, D. 2016. Biometrics in healthcare. *Biometric Technology Today,* 14(9), pp. 9-11.

Marshall, C. & Rossman, G.B. 2016. *Designing Qualitative Research* (6th ed). Sage.

Mason, J. 2018. *Qualitative researching* (3rd edition). London: Sage.

Maxfield, M. & Babbie, E. R. 2018. *Research methods for criminal justice and criminology* (8th edition). Boston, MA: Cengage Learning.

Maxfield, M.G., Babbie, E.R. & Schuck, A.M. 2011. *Research methods for criminal justice and criminology*. Belmont, CA: Wadsworth Cengage Learning.

McKinsey Global Institute. 2015. Digital America: A tale of the haves and have- mores. McKinsey Quarterly. Available at: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/digital-america-a-tale-of-the-haves-and-have-mores (Accessed on 23 April 2023).

Morrow, S. L. 2015. Quality and Trustworthiness in Qualitative Research in Counselling Psychology. *Journal of Counseling Psychology*, 52(2), pp. 250 - 260.

Mudiri, J.L., 2013. Fraud in mobile financial services. *Rapport technique, MicroSave*, *30*.

Mukherjee, S.P. 2020. *A guide to research methodology: An overview of research problems, tasks and methods.* New York: CRC Press Taylor.

Murimbika, S. 2024. Surveying the reputation-regulation interface in the SABI industry: Perspectives of private banking customers. *South African Journal of Business Management*, 55(1), p.3901.

National Treasury. 2020. *Fraud Prevention Plan*. Pretoria: Government Printer.

Nayab, N. 2020. How to determine validity in qualitative research. Project management methods and ideologies. USA: Bright Hub PM.

Ndlovu., N. 2023. News Central Media. Banking app kidnappings: SABRIC on how not to become a victim. TechCentral asked SABRIC-CEO Nischal Mewalall about banking app kidnappings and how people can protect themselves. Available at: https://techcentral.co.za/banking-app-kidnappings-SABRIC-victim/234994/ (Accessed on 22 February 2023).

Noble, H. & Smith, J. 2015. Issues of validity and reliability in qualitative research. *Evidence-Based Nursing,* 18(2), pp. 34 - 35.

Ojo, T. & Adewanmi, A. 1982. *Banking and finance in Nigeria.* Lagos: CIBN & Landmark.

Omar, N. & Bakar, K.M.A. 2012. Fraud prevention mechanisms of Malaysian government-link companies: an assessment of existence and effectiveness. *Journal of Modern Accounting and Auditing, 8*(1), pp. 15-31.

Ombudsman for Banking Services. 2022. New wave of fraud targeting banking customers. Available at: https://www.obssa.co.za/press_releases/new-wave-of-fraud-targeting-bank-customers/ (Accessed on 29 May 2023).

Open Data Charter. 2018. *Using data to combat corruption*. https://open-datacharter.gitbook.io/open-up-guide-using-open-data-to-combatcorruption/background-charter-open-up-guides (Accessed on 14 April 2022).

Organisation for Economic Co-operation and Development. 2013. Managing conflict of interest in the public service: OECD guidelines and country experiences. Paris.

Organisation for Economic Co-operation and Development. 2023. Corruption affecting the public services: OECD guidelines and country experiences. Paris.

Padgett, M. Y. 2015. Perceptions of Nepotism Beneficiaries: The Hidden Price of Using a Family Connection to Obtain a Job. *Journal of Business and Psychology*, 30(2), pp. 283 - 298.

Panigrahi, S., Kundu, A., Sural, S. & Majumdar, A. K. 2007. Use of dempster-shafer theory and Bayesian inferencing for fraud detection in mobile communication networks, in: *Information Security and Privacy*. Springer.

PASA. 2016. Card fraud 2016: protect your card and information at all times. Available at: https://www.SABRIC.co.za/media/1038/2016-card-fraudbooklet.pdf (Accessed 24 April 2022).

Patidar, R. & Sharma, L. 2021. Credit card fraud detection using neural network. *International Journal of Soft Computing and Engineering,* 1(2), pp. 2231-2307.

Pickett, K.S. and Pickett, J.M. 2002. *Financial crime investigation and control*. John Wiley & Sons.

Pieter, B. 2022. *Digital Transformation in South Africa's banking industry*. Available at: https://www.sovtech.co.za/blog/digital-transformation-in-south-africas-banking-industry (Accessed on 14 January 2023).

Prabakaran, M. 2014. *A Multi-Variant Relational Model for Money Laundering Identification using Time Series Data Set. Int. J. Eng. Sci*, 3, pp. 43–47.

Prabhakar, S, Ross, A. & Jain, A.K. 2004. An introduction to biometric recognition*., IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), pp. 4-20.

PricewaterhouseCoopers. 2014. *PwC 2014 Global Economic Survey. Confronting the changing face of economic crime. 4th South African ed*. Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 16 June 2022).

PricewaterhouseCoopers. 2019. *PwC 2019 Global Economic Survey. Confronting the changing face of economic crime 4th South African ed*. Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 16 June 2022).

PricewaterhouseCoopers. 2020. *PwC 2020 Global Economic Survey. Confronting the changing face of economic crime 4th South African ed.* Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 16 June 2022).

PricewaterhouseCoopers. 2022. *Global Economic Survey. Confronting the changing face of economic crime 4th South African ed*. Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 08 March 2023).

Priezkalns, E. 2019. *Mobile Money Fraud Advice Issued by GSMA*. Available at: https://commsrisk.com/mobile-money-fraud-advice-issued-by-gsma/ (Accessed on 23 March 2023).

Rafaiee, R., Olyaee, S. and Sargolzaiee, A. 2013. The relationship between the type of crime and drugs in addicted prisoners in zahedan central prison. *Int J High Risk Behave Addict*, 2(3), pp. 139 - 140.

Rajput, Q., Khan, N.S., Larik, A. & Haider, S. 2014. Ontology Based Expert-System for Suspicious Transactions Detection. *Comput. Inf. Sci.* 7(1), pp. 103 - 114.

Realini, C. 2021 Securing Mobile Money to Deliver on the Promise. Available at: http://www.pymnts.com/asse ts/Lydian Journal/L ydianJournalFebTech.pdf (Accessed on 12 March 2023)

Reilly, D.A., 2019. *Finding the truth with criminal investigation: suspect, subject, defendant*. Rowman & Littlefield.

SABRIC Report. 2021. Deterring and Detecting Financial Reporting Fraud: A Platform for Action. Available at: http://www.thecaq.org/deterring-and-detecting-financial-reporting-fraud (Accessed on 11 June 2023).

SABRIC. 2018. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).

SABRIC. 2019. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).

SABRIC. 2020. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).

SABRIC. 2021. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).

SABRIC. 2022. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 23 August 2023).

Salkind, N. J. 2014. *Statistics for People Who (Think They) Hate Statistic* (5th edition). SAGE Publications.

Saunders, M., Lewis, P. & Thornhill, A. 2019. *Research methods for business students* (8th edition). Essex: Pearson Education Limited.

Sekhu, K. 2023. Banking App kidnappings are on the rise in South Africa. Available at: https://www.kaya959.co.za/lineup/959-breakfast/banking-app-kidnappings-are-on-the-rise-in-south-africa / (Accessed on 12 March 2024).

Seleka, N. 2018. Minister Senzo Mchunu tells court how his SIM card was cloned to extort money from his contacts. News 24. April 21. Available at: https://www.news24.com/news24/southafrica/news/minister-senzo-mchunu-tells-court-how-his-sim-card-was-cloned-to-extort-money-from-his-contacts-20230421 (Accessed on 20 September 2023).

Sharma, A. & Panigrahi, P. K. 2013. A review of financial accounting fraud detection based on data mining techniques. *International Journal of Computer Applications*, 39(1), pp. 37 - 47.

Shulzhenko, N. and Romashkin, S., 2020. Internet fraud and transnational organized crime. *Juridical Tribune*, *10*(1), pp.162-172.

Singh, P. & Singh, M. 2015. Fraud Detection by Monitoring Customer Behavior and Activities: Tenth International Conference on. IEEE. 111(11), pp. 23 - 32.

Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104, pp.333-339.

Solin, M & Zerzan, A. 2010. Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2012/03/amlfinal35.updf. (Accessed on 18 February 2023).

Staff Reporter. 2023. Banking Apps are at the Centre of South Africa's Worrisome Abduction Surge. Available at: https://weetracker.com/2023/11/07/banking-apps-crime-south-africa/ (Accessed on 18 February 2023).

Sukhera, J. 2022. Narrative reviews: flexible, rigorous, and practical. *Journal of graduate medical education*, 14(4), pp. 414-417.

Sun, L., Srivastava, R. P. & Mock, T. J. 2016. An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *J. Manag. Inf. Syst*, 22, 109–142.

Thiel, D. 2016. *iOS application security: The definitive guide for hackers and developers*. No Starch Press.

Tobbin, P. 2021. Understanding mobile money ecosystem: ROLES, structure and strategies, in: *Mobile Business (ICMB),* 2021 Tenth International Conference on. IEEE, pp. 185–194.

Turvey, B. E. 2013. *Criminal Profiling.* Sitka: Elsevier.

Turvey, B.E. and Crowder, S., 2017. *Forensic investigations: An introduction*. Academic Press.

United Nations. 2018. Asset and interest disclosure systems. Conference of the States Parties to the United Nations Convention against Corruption, 5-7 September. Geneva

United States Agency for International Development.2017. Accountability and anti-corruption. Available at: https://www.iisd.org/funders/united-states-agency-international-development-usaid?gad_source=1&gad_campaignid=22208053183&gclid=EAIaIQobChMIlu_coqa3jQMV6plQBh2RGARvEAAYASAAEgKSz_D_BwE (Accessed on 12 April 2019).

Vijayan, J. 2014. Corporate America Slow to Adopt Biometric Technologies. Available at: https://www.computerworld.com/article/1725000/corporate-america-slow-to-adopt-biometric-technologies.html (Accessed on 12 May 2023).

Vithal, R. & Jansen, J. 2019. *Designing your first research proposal: A Manual for Beginning Researchers* (2nd edition). Cape Town: Juta Company [Pty] Ltd.

Wells, J. 2015. *Principles of fraud examination*. New York: John Wiley and Sons.

Wells, J.T., 2017. *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons.

Welman, C., Kruger, F. & Mitchell, B. 2011. Research Methodology, 10th impression. In: I.I. Setlhodi (Ed). Values-Centered Leadership: Insights from Schools that Underperform. Oxford University Press.

Wewege, L., Lee, J. & Thomsett, M.C. 2020. Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, 10(6), pp.15-56.

Yager, R. R. 1987. On the Dempster-Shafer models and new combination rules. *Inf. Sci,* 41, pp. 93–137.

Yin, R.K. 2018. *Case study research and applications: Designs and methods (*6th edition). Los Angeles, CA: Sage.

Zengan, G. & Mao, Y. 2017. A model for data mining-based anti-money laundering research. *J. Money Laund. Control*, 10, pp. 170–179.

Zinn, R.J. & Dintwe, S.I. 2015. *Forensic investigation: Legislative Principles and Investigative Practice*. Cape Town: Juta.

ANNEXURE A: DOCTORAL DEGREE (PhD) BY PUBLICATIONS

Publications: Accredited Journal - Papers related to this study

- Marakalala, Mokopane Charles, Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud (July 18, 2023). OIDA International Journal of Sustainable Development, Vol. 16, No. 05, pp. 19-30, 2023, Available at SSRN: https://ssrn.com/abstract=4675020
- Marakalala, Mokopane Charles, Forensic Analyst: The Impact of Human Trafficking and Modern Slavery at Schools and Campuses in African Union (December 14, 2023). OIDA International Journal of Sustainable Development, 17 (08), 11-22, 2024., Available at SSRN: https://ssrn.com/abstract=4871833
- Marakalala, Mokopane Charles, Forensic Identification: The Biometric Technology Linked to Online Financial Fraud and Crime Related to the South African Banking Industry (August 27, 2024). OIDA International Journal of Sustainable Development, 17 (12), 81-98, 2024, Available at SSRN: https://ssrn.com/abstract=5012581
- Marakalala, Mokopane Charles, Forensic Identification: The Biometric Technology Linked to Online Financial Fraud and Crime Related to the South African Banking Industry (August 27, 2024). OIDA International Journal of Sustainable Development, 17 (12), 81-98, 2024, Available at SSRN: https://ssrn.com/abstract=5012581
- Marakalala, Mokopane Charles and Matlala, Mpho Mark, Border Management Identification: The Biometric Technology to Detect Criminals and Terrorists Often Travel using Falsified Identity Documents (August 26, 2024). OIDA International Journal of Sustainable Development, 17 (12), 57-70, 2024., Available at SSRN: https://ssrn.com/abstract=5012581
- Marakalala, Mokopane Charles, Forensic Expert: An analysis of the solution in the App Kidnappings links to financial fraud in South Africa banking industry Research World / 11 January 2025. Access Link: https://mg.co.za/research-world-papers/2025-01-11-forensic-expert-an-analysis-of-the-solution-in-the-app-kidnappings-links-to-financial-fraud-in-south-africa-banking-industry/
- Marakalala, Mokopane Charles and Mothapo, Mahlodi, Evaluating the Success of South African Law Enforcement in Combating Drug and Substance Abuse: Are we Winning the Fight? The Case study of Youth-Network Engaged Scholarship Project (December 04, 2024). OIDA International Journal of Sustainable Development, 18 (09), 85-98, 2025, Available at SSRN: https://ssrn.com/abstract=5259526

Published articles in accredited journals (within the last 5 years)

- M C Marakalala, R J Mokwena, Forensic Investigation: The Impact of Money-Laundering During Lockdown in South Africa, International Journal of Social Science Research and Review: Vol 6 No 1 (2023): IJSSRR VOL 6 NO 1 2023 JANUARY
- M C Marakalala, Forensic Investigation: The Case of Procurement Fraud in Madibeng Local Municipality (Northwest Province), International Journal of Social Science Research and Review: Vol 6 No 2 (2023): IJSSRR VOL 6 NO 2 2023 FEBRUARY
- Marakalala, M. C. (2025). The Engagement Vision of Basic Education as an Asset for Social Justice in South Africa and African Community. Review of Law and Social Sciences, 3(2), 11–26. https://doi.org/10.71261/rlss/32.1126

Published chapters in book for the subject specialists

- Marakalala, Mokopane Charles, Forensic Expert: An exploration of Challenges Encountered by the Forensic Investigators in the Investigation of Mobile Fraud in the South African Banking Industry https://gbata.org/wp-content/uploads/2025/01/GBATA-2024-Readings-Book.pdf
- Governance and Public Leadership: Corruption, Social Security and Ethics/Ubuntu in the South African and African Communities https://gbata.org/wp-content/uploads/2025/01/GBATA-2024-Readings-Book.pdf

Textbook in progress related to study

- Forensic Subject Matter: Online Financial Fraud and Commercial Crime Investigation
    - ❖ Publisher: Juta (2024-2025)

ANNEXURE B: ETHICAL CLEARANCE

College of Law_RERC

Date: 30/10/2023

Ref #: 2023

Name: Mr Mokopane Charles Marakalala

Student #: 46691022

Dear: Mr Mokopane Charles Marakalala

Decision: Ethics Approval from

Researcher: Mr Mokopane Charles Marakalala

40334 Mamelodi West
Pretoria
0122
marakmc@unisa.ac.za
0760620021

Supervisor: Dr AC Madzivhandila 36505080@mylife.unisa.ac.za

Ethics application-MC Marakalala

Qualification: Doctor of Philosophy in Criminal Justice Police Science, Forensic Science and Technology

_____

_____

Thank you for the application for research ethics clearance by the College of Law_RERC for the above-mentioned research study Ethics approval is granted for three years.

The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of
conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.

Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.

No field work activities may continue after the expiry date 30/10/2026. Submission of a completed research ethics progress report will constitute an application for renewal, for Ethics Research Committee approval.

Additional Conditions

Disclosure of data to third parties is prohibited without explicit consent from Unisa.
De-identified data must be safely stored on password protected PCs.
Care should be taken by the researcher when publishing the results to protect the confidentiality and privacy of the university.
Adherence to the National Statement on Ethical Research and Publication practices, principle 7 referring to social awareness, must be ensured: "Researchers and institutions must be sensitive to the potential impact of their research on society, marginal groups or individuals, and must consider these when weighing the benefits of the research against any harmful effects, with a view to minimising or avoiding the latter where possible." Unisa will not be liable for any failure to comply with this principle.
Note

The reference number 2023 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Kind regards,



Prof Lincoln Fitz
Chair of College of Law_RERC
E-mail: fitzlg@unisa.ac.za



Executive Dean / By delegation from the Executive Dean of College of Law_RERC
E-mail: koleoj@unisa.ac.za

ANNEXURE C: LANGUAGE AND TECHNICAL EDITOR CERTICATE OF COMPLETION

The Best Language Nurturer
ENGLISH & AFRIKAANS LANGUAGE SERVICES
COPY EDITING etc.

Cell: 082 2025 167 | Email: maryna.roodt@gmail.com

EDITOR'S DECLARATION

11-Sep 2025

To whom it may concern:

I, Maryna Roodt, an independent freelance language practitioner, hereby declare that I was tasked to carry out the language editing of the following dissertation:

AN EXPLORATION OF BIOMETRIC-BASED SOLUTION IN COMBATING MOBILE FRAUD AT SOUTH AFRICAN BANKING RISK INFORMATION CENTRE

Written by: **Mokopane Charles Marakalala**

Student name: **Mokopane Charles Marakalala**

Student number: **46691022**

Which is submitted in accordance with the requirements for the degree of:

DOCTOR OF PHILOSOPHY IN CRIMINAL JUSTICE

After my initial editing, several updates of the entire document were carried out by means of a "question and answer" exercise to render the work as error-free as possible. Please note that I take no responsibility for any alterations and/or errors that were introduced to the document after I finally returned it to the author.

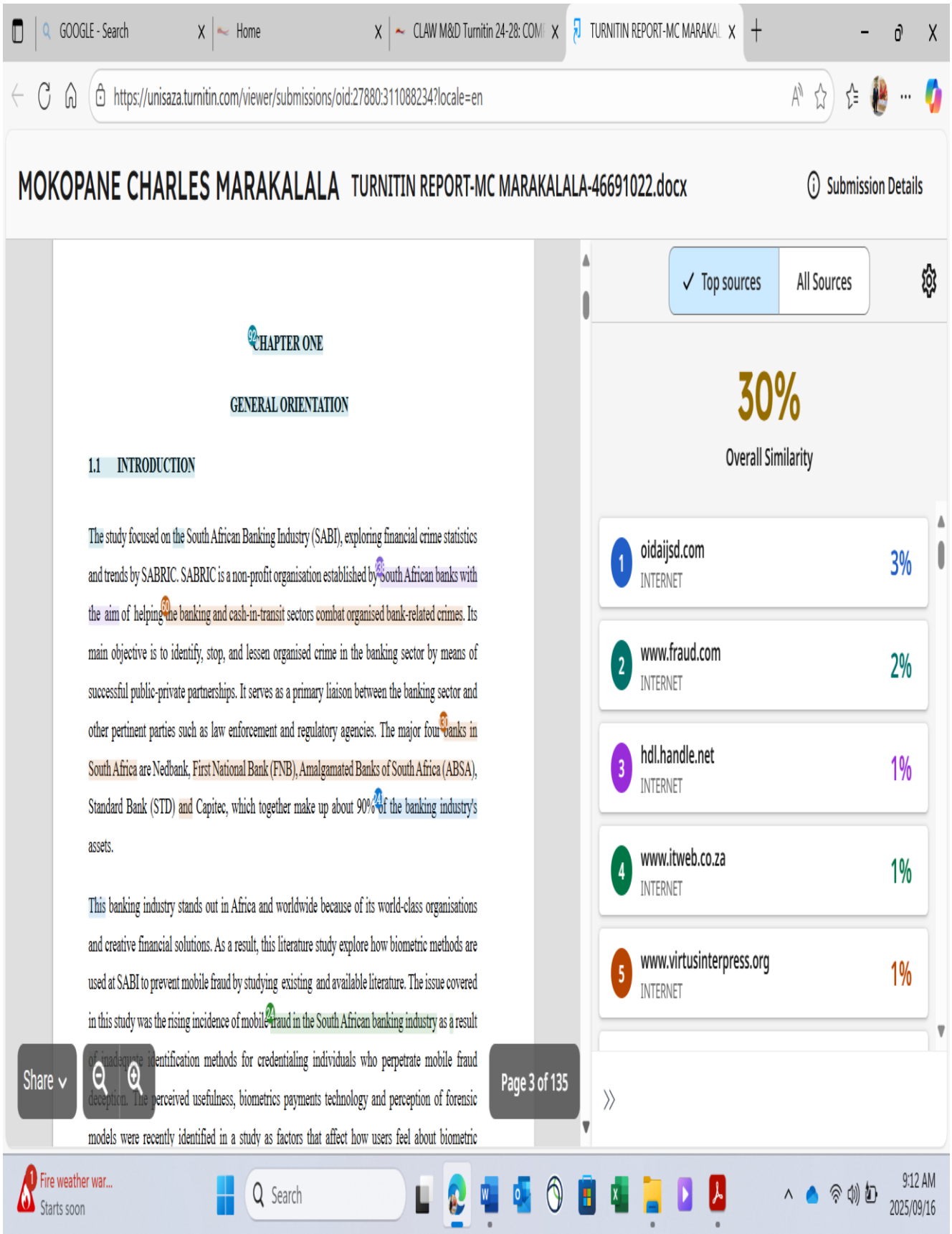
I have extensive experience in copy- editing and have the following qualifications:
BA (major in English); Hons (BA) (English); MA(Applied Linguistics)
and MA (Higher Education Studies).

MP Roodt

MP Roodt
maryna.roodt@gmail.com
082 202 5167

The Best Language Nurturer

ANNEXURE D: TURNITIN DIGITAL RECEIPT



ANNEXURE E: SABRIC MAP LOCATION

