



**Developing an intelligence and security framework to counteract insurance
fraud in the low income sector. The case of Zimbabwe.**

by

SOUL NYANGONI

219015542

A thesis submitted in fulfilment of the requirements for the degree

Of

Doctor of Business Administration

Graduate School of Business and Leadership

College of Law & Management

Supervisor: Prof Bibi Zaheenah Chummun

Date: 2 December 2022

DECLARATION

I Soul NYANGONI, DBA student at University of KwaZulu Natal declare the following:

That this research, reported in this thesis is my sole original work. The thesis has not been submitted for any other university's degree or examination or any related academic work. Also prudent to note is that this thesis is purely my work and other information which may include data, graphs and pictures obtained from other external sources were acknowledged. Material copied and pasted from the internet was also excluded from this thesis unless specifically acknowledged, and the source being detailed in the thesis references section. Where exact there has been direct citation, such writing has been placed inside quotation marks, and referenced accordingly.

In light of the above, I confirm that the thesis I am submitting is an original and authentic thesis that satisfies UKZN regulations with regards to plagiarism. I further confirm that I have fully referenced all material in this thesis in accordance with the Havard system.



Soul Nyangoni

2/12/2022

Date

ACKNOWLEDGEMENTS

Intelligence, a world that rules the world.

I acknowledge the men and women across the globe who risk their lives and lives of loved ones collecting vital intelligence to protect their countries, with special recognition to my father Gilbert Nyangoni who spent thirty-two (32) of his life in the Zimbabwe Intelligence Corps, a division of the Military Intelligence Directorate.

My family, my mother Rosemary, two sisters Shinga and Sakhile and my two children Aimee and Gildert, it was not going to be possible without their love, support and encouragement throughout this remarkable academic journey. I also acknowledge unwavering and resilient support from my best friend and companion. My wife Gamuchirai.

This would have not been possible without the guidance and instruction from the best supervisor ever. This supervisor has changed lives in this world through knowledge sharing and my prayer is that God grants her wishes of her life. Dr Bibi, you great and outstanding. Thank you.

Staff at the Insurance and Pension Commission (IPEC), members of the Zimbabwe intelligence community. The insight, knowledge and information you shared and you bestowed on me contributed immensely to the success of this thesis.

ABSTRACT

This study explores avenues to develop a security and intelligence framework to counteract insurance fraud in the low-income sector in Zimbabwe. Insurance fraud, a threat to both national security and performance of the micro insurance industry, offering insurance services to low-income earners in Zimbabwe. The examination stretches from the causes of micro-insurance fraud to measures that can be fused with security intelligence to combat micro-insurance fraud. The framework of this study was a quantitative study, following stratified random sampling of three hundred and twenty-six participants. A structured questionnaire was deployed to collect primary data and complemented by interviews, focus groups and document inspection. The association between causes of insurance fraud, organised criminal syndicates, and low-income earners were investigated using structural equation modelling. The primary objective was to identify factors that enhance insurance fraud and measure the significance and causal effect of the identified variables. The response postulated that there are internal and external factors amongst them poor internal controls, lack of investment in artificial intelligence and poor human capital management systems which are being explored by organised crime syndicates to peddle micro insurance fraud. The internal and external factors work as an integrated front and the absence of one factor may negatively affect the decision to continue with the crime. In that regard, this study recommended the CEPSI strategy. The acronym CEPSI abbreviates for Customers, Employees, Participation, Systems and Intelligence and this is meant to overhaul micro-insurance service provider's operating systems. Conclusions were reached after synchronisation of primary and secondary data with research objectives. The CEPSI approach provide insurance firms with capabilities to detect, prevent, sanction, investigate, and remediate insurance fraud in the low-income sector of Zimbabwe. The focus is to equip the micro-insurance service providers with proactive capabilities meant to detect and thwart insurance fraud amongst policyholders, employees and organised crime syndicates by designing internal security measures fused with artificial intelligence to detect insurance fraud, educating the general public with regards to threats and consequences of insurance fraud and also working in liaison with security intelligence apparatus.

Keywords: Insurance Fraud, Low Income Earners, Organised Crime, Security Intelligence,

TABLE OF CONTENTS

Contents	Pages
DECLARATION.....	i
ABSTRACT.....	iii
LIST OF TABLES.....	x
LIST OF FIGURES.....	xi
GLOSSARY OF ACRONYMS.....	xii
CHAPTER ONE.....	1
INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Background of the Study.....	1
1.3 Research Problem.....	4
1.4 Research Objectives.....	8
1.5 Research Questions.....	9
1.6 Conceptual Framework.....	9
1.7 Research Design and Methodology.....	11
1.7.1 Unit of analysis and sampling.....	11
1.7.2 Data collection.....	12
1.7.3 Data Analysis.....	13
1.8 Significance of the Study.....	13
1.9 Scope of the Study and Chapter Outline.....	14
1.10 Structure of the Thesis.....	16
1.11 Chapter Summary.....	17
CHAPTER TWO.....	18
Threat of Insurance Fraud in the Low Income Sector and Role of Security Intelligence.....	18
2.1 Introduction.....	18
2.2 What is Insurance?.....	19
2.2.1 Micro Insurance.....	23
2.3 Definition of Insurance Fraud.....	35
2.4 Organised Crime Syndicates and Insurance Fraud.....	36
2.5 The Fraudster.....	42
2.6 Cost and Threats of Insurance Fraud.....	49
2.6.1 Cost of insurance fraud.....	49

2.6.2 Health Insurance Statistics.....	51
2.6.3 Automotive Insurance Fraud	52
2.6.4 Scams in Life Insurance	53
2.6.5 Statistics on Property and Disaster Insurance Fraud	54
2.7 Threat of Insurance Fraud.....	54
2.8 Consequences of Insurance Fraud	57
2.9 Insurance in Developing Economies	58
2.10 Micro Insurance and Human Security.....	60
2.11 Overview of the Zimbabwean Insurance Industry.....	64
2.12 Low-income and Micro Insurance.....	69
2.13 Types of Insurance Fraud in Zimbabwe	72
2.13.1 Internal Insurance Fraud.....	73
2.13.2 External Insurance Fraud	76
2.13.3 Intermediary Insurance Fraud	76
2.13.4 Opportunist Fraud.....	78
2.13.5 Syndicate Fraud.....	78
2.14 State of Security Countermeasures in the Micro Insurance Sector.....	79
2.15 Insurance Regulation	81
2.15.1 The Insurance and Pension Commission	92
2.15.2 The board of the Insurance and Pension Commission's (IPEC)	93
2.15.4 Functions of the Insurance and Pension Commission's (IPEC)	94
2.15.5 The Insurance Bill	95
2.15.6 Pension and Provident Funds Bill [Chapter 24:09]	96
2.15.7 The Zimbabwe Anti-Corruption Commission.....	98
2.16 Insurance Intermediaries	102
2.17 Role of Security Intelligence Organisation in Countering Insurance Fraud	104
2.17.1 Intelligence Cycle and Counter Insurance Fraud	107
2.17.2 Taking action:	109
2.18 The Missions of Intelligence.....	110

2.19 Tradecraft.....	111
2.20 Agent Acquisition and Handling.....	112
2.20.1 Establish the requirement	113
2.20.2 Finding a potential source.....	114
2.20.3 Assessing suitability	114
2.20.4 The approach and recruitment.....	114
2.20.5 Running the source	115
2.20.6 Recording the operation	115
2.20.7 Termination and resettlement.....	115
2.21 Profiling	115
2.22 Surveillance and Counter Organised Crime.....	117
2.22.1 Electronic surveillance	118
2.22.2 Static surveillance	118
2.22.3 Mobile surveillance.....	119
2.22.4 Tracking.....	119
2.23 Undercover Operations	119
2.24 Conclusion.....	120
CHAPTER THREE	121
THEORETICAL REVIEW	121
3.1 Introduction	121
3.2 Fraud Triangle	122
3.2.1 Pressure	122
3.2.2 Perceived Opportunity.....	124
3.2.3 Rationalisation	125
3.2 Shortcomings of the Fraud Triangle.....	126
3.3 Adam’s Equity Theory	127
3.4 Theory of Reasoned Action.....	130
3.5 Rational Choice Theory	132
3.6 Deterrence Theory	135
3.7 Chapter Summary	137

CHAPTER FOUR.....	139
RESEARCH METHODOLOGY	139
4.0 Introduction	139
4.1 Research Philosophy	140
4.2 Research Design	142
4.3 Quantitative Research.....	143
4.4 Participants and Sample Size	144
4.4.1 Participants	144
4.4.2 Sampling and Target Population.....	145
4.5 Data Collection Techniques	148
4.5.1 Questionnaire	149
4.5.2 Administration of the questionnaire	150
4.6 Test Run	152
4.7 Interviews and focus group discussions.....	152
4.8 Documents inspection	153
4.9 Research Objectives and Methodology	155
4.10 Data Analysis	156
4.10.1 Correlation Analysis	156
4.10.2 Structural Equation Modelling.....	158
4.10.3 Reliability and Validity.....	159
4.10.5 Bias Reduction.....	161
4.11 Ethical Issues	162
4.12 Chapter Summary	165
CHAPTER FIVE	167
DATA ANALYSIS	167
5.1 Introduction	167
5.2 Presentation of Results	167
5.2.1 Area Coverage.....	168
5.2.2 Questionnaire Responses	169
5.2.3 Industry Coverage	170
5.2.4 Socio-Demographics	172

5.4 Factors Enhancing Insurance Fraud	172
5.5 Analysis of Behavioural Responses	182
(Sources: Owners Compilation)	183
5.6 Confirmatory Factor Analysis	183
5.7 Total effects	188
5.9 Model fit.....	189
5.9.1 Cronbach Alpha	191
5.10 Chapter Summary	192
CHAPTER SIX	194
DISCUSSION OF FINDINGS	194
6.1 Introduction	194
6.2 Profile of Low Income Earners	194
6.3 Findings Related to Types of Insurance Fraud	198
6.4 Findings on Factors Enhancing Insurance Fraud	201
6.5 Findings on Organised Crime Syndicates Operations in the Insurance Industry	206
6.6 Findings on Insurance Companies Targeted by Organised Crime Syndicates	208
6.7 Findings Regarding Legislation to Counter Insurance Fraud	209
6.9 Findings with Regards to the Role of Security Intelligence in Countering Insurance Fraud	210
6.10 Conclusion	212
CHAPTER SEVEN.....	213
CONCLUSION AND RECOMMENDATIONS	213
7.1 Introduction	213
7.2 Main Findings and Conclusions of the Study	213
7.2.1 Research Conclusion Conceptual Framework.....	213
7.2 Recommendations	215
7.2.1 Customer /Policyholder	219
7.2.1.1Profiling and validation	220
7.2.1.2 Criminal Clearance	220
7.2.1.3 Vetting.....	221
7.2.1.4 Awareness.....	221
7.2.1.5 Incentivising	222
7.3 Employees.....	222

7.3.1 Employee Training and Development.....	223
7.4 Participation in Awareness	225
7.5 Systems	226
7.5.1 Artificial Intelligence Systems	226
7.5.2 Internal Control Systems.....	228
7.6 Intelligence.....	230
7.7 Limitations.....	233
7.8 Conclusion.....	234
REFERENCES	236
APPENDICES	261
Appendix A: Informed Consent Form	261
Appendix B: Questionnaire	263
Appendix C: Editorial Letter	276
Appendix D: Gatekeeper Letter	277
Appendix E: Ethical Clearance.....	278

LIST OF TABLES

Table 2.2: Claims fraud survey	80
Table 4.1: Stratified sample per region.....	147
Table 4.1: Data Collection Techniques.....	154
Table 4.2: Linkage between Methodology and Research Objectives.....	155
Table 4.3: Ideal spectrum for interpreting correlation coefficient.....	157
Table 4.4: Types of Bias	162
Table 5.1: Survey Questionnaire Breakdown	169
Table 5.2: Likert Scales Responses	183
Table 5.5: Regression Weights	187
Table 5.6: Total Effects.....	189
Table 5.6: The Model.....	190
Table 5.7: Scale reliability and validity statistics	192
Table 6.1: Frequencies: Insurance fraud a threat to national security and interest.....	196
Tables 6.2 and 6.3: External and Internal Factors Enhancing Insurance Fraud.	201

LIST OF FIGURES

Figure 2.2: The fraudster cycle	48
Figure 2.3: Micro insurance distribution channels	68
Figure 2.4: Intelligence cycle.....	108
Figure 3.1: Fraud triangle	122
Figure 4.1: A Framework for Research—the Interconnection of Design, and Research Methods.....	141
Figure 4.3: Stages of planning a questionnaire	149
Figure 4.4: Various forms of validity	160
Figure 5.1. Provinces of Zimbabwe	168
(Source: Zimbabwe Surveyor General: 2020)	168
Figure 5.2: Industry coverage	171
Figure 5.3: Gender and Race	172
Figure 5.4: Respondents rate on external factors.....	173
Figure 5.4: Respondents rate on internal factors	179
Figure 5.5: Structural model with unstandardized regression weights	185
Figure 6.1: Types of Insurance Fraud.....	200
Figure 6.2: External Factors Enhancing Insurance Fraud.....	204
Figure 6.3: Internal Factors Enhancing Insurance Fraud.....	206
Figure 7.1 Research Conclusions Conceptual Framework	215
Figure 7.2: Customers, Employees, Participation, Systems and Intelligence 360.....	218

GLOSSARY OF ACRONYMS

AI	Artificial Intelligence
CBZ	Commercial Bank of Zimbabwe
CEPSI	Customer, Employees, Policies, Systems and Intelligence
CFA	Confirmatory Factor Analysis
CID	Criminal Investigation Department
CID	Criminal Investigation Department
IAIS	International Association of Insurance Supervisors
IPEC	Insurance and Pensions Commission
PD	President's Department
POSB	People Own Bank
SEM	Structural Equation Modelling
TOCS	Transnational Organised Crime Syndicates
ZACC	Zimbabwe Anti-Corruption Commission
ZMFED	Zimbabwe Minister of Finance and Economic Development
ZNA	Zimbabwe National Army
ZRP	Zimbabwe Republic Police
USA	Unites States of America
IAIS	International Association of Insurance Supervisors

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The threat of insurance fraud in insurance companies offering services to low-income earners, a concept interchangeably referred to as micro-insurance fraud has received attention from various researchers, governments, insurance experts, forensic investigators, law enforcement agents and intelligence officers around the world, with Africa taking a leading position in terms of escalating insurance fraud cases targeting low-income earners and their micro insurance service providers. This has been necessitated by micro-insurance fraud being categorised as a serious crime and a public social issue globally and, hence the crime requiring proactive prevention and countermeasures (Jung & Jik-Kim, 2021).

This study's first chapter, chapter one provides an overall picture of the study, giving an introduction, against the backdrop of considerations that initiated this study. It defines the study in terms of issues under examination as well as the research objectives. Following that, an overview of the study methodology and data analysis approaches that the researcher considered to be appropriate to solve the research problem is offered. There is also a summary of major terms and topics used in this study. Following that, the chapter closes by laying out the groundwork for the research's structure.

1.2 Background of the Study

The departing point for insurance experts, policymakers and intelligence officers in Zimbabwe is to understand what micro insurance is and its importance to the previously excluded low-income earners group. Various definitions exist concerning what is micro insurance, amongst them, the International Association of Insurance Supervisors (IAIS), have provided one of the most universally accepted definitions of microinsurance that appeals to the academic, business community and security intelligence sectors. Micro insurance, according to the IAIS (2018), is the protection of low-income people against specific risks in exchange for recurring premium payments based on the likelihood and expense of the risk involved. The word micro related to servicing a certain income sector in emerging market countries, according to the IAIS (2018). This was on the realisation that low-income earners in less economically developed economies have limited access to various insurance services

such as health care services and funeral cover while they mostly live and work in environments that pose a serious risk to their livelihoods, susceptible to theft, accidents and illnesses, all this is combined with limited income to afford insurance and even localised safety nets. Furthermore, low-income earners in the informal, private, and public sectors are exposed to a variety of risks that threaten and pose a real risk to their savings, which may take the form of assets and domestic animals that are classified as wealth but frequently managed with insufficient informal, perceived insurance measures and tools.

Microinsurance is, in principle, the same as any other type of insurance. The only distinction is that microinsurance is aimed at low-income individuals who in Zimbabwe, regardless of industry or economic sector, have little, limited financial reserves and revenues that fluctuate greatly. The size of the premium and the covered amount are the main differences between traditional insurance and micro insurance. Microinsurance rates are typically known to be cost-effective, and cheap, and other insurance companies have accepted periodic installments payments to account for the policyholder's variable sources of income. In essence, the insurance business has become more inventive, with insurance companies, in particular, micro insurers, increasingly turning to the novel, tailor-made services that are all-encompassing and satisfy the needs of the target market of low-income workers.

Insurance fraud since the inception of microinsurance services has been a significant problem for insurers and a threat to insurance companies offering services to low-income earners. The United States of America, Association of Certified Fraud Examiners (2017) viewed insurance fraud in this specific market as the most widespread form of fraud internationally. Further, the United States of America, Association of Certified Fraud Examiners (2017) categorised insurance fraud being the most prevalent crime, second only to tax fraud. An examination of criminal documentation of insurance fraud in insurance companies offering services to low-income earners in Zimbabwe has indicated that organised crime syndicates, employees and insurance experts acting in isolation or as accomplices involved in organised micro insurance fraud crimes have also gone innovative. Their criminal activities have since been fused with technology, while their modus operand has changed from static to mobile and highly concealed. Organised crime groups have constantly pursued weaknesses within individual insurance companies and the industry at large. When micro insurance fraud countermeasures are tightened in one area, they have scouted for lax security opportunities to exploit in another area. According to the Insurance Europe Report (2019), insurance fraud is constantly

evolving, shaped by the technology at the organised crime syndicates' disposal. Cyber-enabled fraud has become more prevalent as more insurance companies conduct business online. Digitisation and the internet of things (IoT) have over the years transformed businesses around the globe including the insurance industry, with finances, assets and services gone digital, shifting from the usual physical, traditional way of doing business (Schwab 2016).

Regardless of the dangers and threats to micro insurance, micro insurance has been considered a tool for extending social security to the typically excluded, low-income earners, particularly in Zimbabwe. According to Loewe and Deblon (2011), internationally, social nets extended to low-income earners, in some countries such as Zimbabwe, described as social protection is a national interest and priority considering that plus seventy-five per cent of the total population is considered low-income householders or earners. Complementary to article twenty-two, the Universal Declaration of Human Rights and article nine, International Covenant on Economic, Social and Cultural Rights (1948), social protection is regarded and treated as a human right since 1948. In that regard, micro-insurance offered coverage or insurance services to low-income earners, be it households or individuals who have little savings, as an innovative tailored social protection net specifically for assets that are recognised as of less value, health, injury and death cover. However, for insurance companies in the low-income market to succeed in offering realistic, serviceable micro insurance products, both the insurance companies for low-income cover and policyholders should benefit from the mutual relations with the insurance company meeting its profit and operational objectives while policyholders receive services in dire cases of vulnerability (Biener & Eling, 2012). The achievement of these two divergent trajectories is constantly being compromised by the rate at which micro-insurance fraud is escalating in the insurance industry, particularly rampant in insurance companies offering cost-effective insurance services and products to low-income earners.

On-going global research on generalised microinsurance fraud is steadily increasing, notably with very thin research on microinsurance fraud in Zimbabwe and other developing economies. Insight into current literature revealed very limited research on the insurance fraud threat, irrespective of the recognition and confirmations that micro-insurance fraud exhibits a potential of becoming an enormous threat compared to general insurance fraud in Zimbabwe (Zimbabwe Anti-Corruption Commission, 2020). The rampant increase of

insurance fraud cases globally is giving diversified challenges to governments and the insurance industry, with some companies and government agencies invested in technology, technical expertise and capabilities to detect, investigate and thwart fraud in general and insurance fraud, in particular, emanating internally or externally. A study of global claims fraud exhibits that three to four per cent filed claims are possibly fraudulent. Coalition against Insurance Fraud (2019) puts the global cost of insurance fraud at eighty billion United States dollars. This, however, excludes costs on anti-fraud controls, compliance, public awareness, artificial intelligence and employee training. According to the Zimbabwe Minister of Finance and Economic Development (ZMFED), Ncube (2020), what is unknown by the general public and other policymakers is that large sums of money paid out by insurance companies owing to insurance fraud weakens the financial position of the company and causes grave consequences to other stakeholders, which may not be limited to the government only. Policyholders have also suffered escalating premiums.

Money obtained from insurance drives organised crime globally, fuelling terrorism and money laundering. Lack of regional cooperation, particularly in Africa, remained one of the obstacles to combating insurance fraud even to date (Moyo, 2019) exposing the ignorance that insurance fraud is one of the greatest threats that have compromised human security. Further, law enforcement agencies, such as the police, lack the protocols to investigate insurance fraud. Faced with the rising frequency and sophistication of insurance fraud coupled with a slow regulatory pace, absence of security intelligence and little artificial intelligence investment by regulatory state entities, insurance companies ought to be one step ahead by working in liaison with state security intelligence apparatus and as well as identifying modern, effective and faster counter insurance fraud measures that could be installed within the insurance company operating systems.

1.3 Research Problem

Diverse forms of fraud in the insurance sector is and has been a serious threat, a crime with socio-economic impact to service delivery, survival and operations of various entities including micro insurers, the entire insurance industry and the economy (Tseng & Su, 2013). In Zimbabwe, the insurance industry is losing annually an excess of one hundred and sixty-five million United States of America dollars to insurance fraud perpetrated by organised crime syndicates. A commissioner at the Insurance and Pension Commission, Karonga (2020), confirmed that the entire insurance industry collects annually about five

hundred and fifty-five million United States of America dollars and thirty per cent is lost annually owing to insurance fraud. The rate at which insurance fraud is escalating with money obtained from this nefarious activity injected to finance other criminal activities has become a national security threat. Terrorism and insurgency groups in Africa are a cause of concern with regional destabilisation being a serious concern amongst security experts. Classified intelligence forecasts and estimates within the Zimbabwe intelligence community, foresee money obtained from insurance fraud financing regional destabilisation in Southern Africa. Regional destabilisation therefore could be heavily financed by organised crime syndicates who could have illegally obtained money through illicit means including insurance fraud (President's Department, 2020). On-going coalition investigations by the government of Zimbabwe's security task force known as the Joint Operations Command (JOC), have so far established that organised crime syndicates are targeting insurance companies offering micro-insurance services. JOC comprises the three-security intelligence apparatus of Zimbabwe, namely the President's Department internally known as the Central Intelligence Organisation (CIO), Zimbabwe National Army (ZNA), Military Intelligence Directorate (MID) and the Zimbabwe Republic Police (ZRP), and Police Internal Security Intelligence (PISI), organised crime syndicates are taking advantage of security loopholes within insurance companies offering services to low-income earners. The security loopholes stretch from non-investment in artificial intelligence, poor internal control systems and the dispatch and payments of insurance services via mobile phone networks without prior security vetting and clearance of the owner of the mobile phone.

The investigations further extrapolated that insurance fraud would not only finance global destabilisation but also destabilise national interest in Zimbabwe considering that it has compromised the development of effective micro-insurance services earmarked for low-income earners. According to a survey conducted by Zimbabwe's National Statistical Agency (2021), ninety-five per cent of the working population in Zimbabwe is classified as low-income earners. According to Zimbabwe's National Statistical Agency (2022), Zimbabwe's population was fifteen million one hundred and seventy-eight thousand as of April 20, 2022, with 7 289 558 (48%) males and 7 889 421 females (52 %). The working population was anticipated to be nine million, accounting for fifty-nine per cent (59%) of the overall population. The largest number, estimated to be four point one million is made up of smallholder farmers in communal agriculture and the informal sector. The outstanding is in

cross-border trading and informal trading. The ministry responsible for capacitating low-income earners in Zimbabwe, the Ministry of Small to Medium Enterprises Development (MSMED), (2019) affirmed that there is an unexplained number of students and individuals who are formally unemployed who contribute to the informal sector. Of this potential workforce, nine hundred and fifty thousand are students while eight hundred thousand are officially defined as unemployed but doubling as the labour force in the informal sector. However, the low-income sector also stretches into the private and public sectors. According to the Public Service Commission (2021), individuals and household units whose income is below the povam datum line, are categorised as low-income earners in Zimbabwe. This category is estimated to be five million employees in the private and public sectors. These employees are one way or the other in need of accessing budget micro-insurance services. Considering the numbers, it is in the interest of the government of Zimbabwe to provide social protection to the above-stated low-income earners since this could jeopardise the possibilities for peace, stability, and long-term development in Zimbabwe.

The social protection measures initiatives fronted by the government to cater for the low-income earner's segment are compromised with most micro-insurance service providers failing to offer the services when requested. This is due to a high level of insurance fraud and the situation further being worsened due to a lack of appropriate countermeasures amongst micro insurance companies. Findings are that microinsurance companies hardly invest in fraud countermeasures; hence organised crime syndicates take advantage of such weaknesses. Furthermore, the Zimbabwe Republic Police since its establishment post-Zimbabwe independence has exhibited a deficiency in resources and capabilities to deal with such highly organised, sophisticated and surreptitious crimes. Mandatorily, the police play a pivotal and crucial role in preserving law and order and protecting the security of residents and the nation. They own arresting powers, and authority to detain, search, and deployment of minimum force to carry out their constitutional mandate. However, police officers in Zimbabwe have frequently abused these duties, resulting in major ramifications for the organisation's image and operations (Mugari & Obioha, 2018). In some cases, members of the Zimbabwe Republic Police are accomplices in organised insurance fraud cases. Preliminary research done so far confirmed that law enforcement agents, which include the police, apart from being corrupt, lacked the capabilities to counter insurance fraud perpetrated by organised crime syndicates who are technologically advanced. However, some research

suggests that once a criminal act becomes a threat to national security and interest, the country's security intelligence apparatus can be deployed to counter such crime. The primary objective of national security intelligence is proactive and through tradecraft, they detect and thwart any form of threat to national security emanating internally or externally.

Imperatively, it is acknowledged by scholars and researchers that the field of security intelligence is a highly secret field and operations of intelligence organisations or agencies have gone undisclosed for a long time. Little is known about the Secret Service and how it can be beneficial to a nation. This research intends to tap into the secrecy and tradecraft or tactics of intelligence operations and operatives in countering organised insurance fraud. Human security, contrary to historical notion by security intelligence apparatus that focused on state security, is not primarily concerned with threats to territorial integrity or acts of aggression against a state as the primary beneficiary of international security but focuses on human security. Governments, the United Nations, insurance experts and intelligence officers around the world believe that the world is insecure, hence compromising human security with several hazards and threats. Prolonged crises, violent conflicts, natural disasters, persistent poverty, diseases, fraud, corruption and economic downturns wreaked havoc on people's lives and jeopardised possibilities for peace, stability, and long-term development. Such crises are complicated as they include a variety of human vulnerabilities. When they collide, they have the potential to spread enormously, triggering mass disturbances and destabilisation in communities and spanning national boundaries. The Zimbabwe intelligence community (2021) adopted the concept of human security from the United Nations, General Assembly resolution 66/290 that human security is an initiative to detect and alleviate broad and cross-cutting problems to the survival, livelihood, and dignity of the people, people-centered, comprehensive, context-specific, and prevention-oriented actions that increase all people's protection and empowerment. Human security brought together a diverse set of actors from the security intelligence apparatus, insurance business, government, private sector systems, civil society, and local communities. This enabled the creation of synergies that take cognisance of multiple stakeholders' comparative advantages. The changing role of an intelligence organisation, moving away from the traditional state-centric, to human-centric security that prompts the security intelligence apparatus to intervene on issues concerning threats to citizens such as micro insurance fraud since they compromise human and national security.

So far there is very limited research on the need to deploy a security intelligence organisation to investigate and counter insurance fraud. Research so far carried out in economically advanced economies for example the United Kingdom has already advocated and initiated deployment of its security intelligence unit, the Military Intelligence Six (MI6) to combat the threat of insurance fraud. Zeroing on developing economies, little, insignificant research done so far has not yet yielded positive results for the insurance industry in terms of containing insurance fraud. The little research done so far has focused more on countering insurance fraud in general without zeroing in on micro-insurance fraud which affects a bigger percentage of the population. In light of this, this study's main objective is to bridge the research gaps identified above, as well as recommend the combining of organisational systems, internal insurance fraud countermeasures with security intelligence in the fight against micro insurance fraud. This research will enlighten more and demystify the misconceptions concerning security intelligence and intelligence operatives. Security intelligence services are usually categorised as dreaded and only deployed to contain and eliminate political rivals. The fact is that security intelligence is a secret, spy organisation whose deployment can be beneficial to a country. As a spy organisation, security intelligence agencies are rather developmental agencies of a state and part of their role is to detect, intervene and thwart threats to national security while a division within the spy organisation such as VIP protection concentrates on providing individual protection to every important people within a state. Though the operations of security intelligence organisations will remain secret, the fact is that intelligence is an arm of the government, and their duties are security and secret in nature, hence they become the most ideal organisation to deal with issues of organised crime. In such particular circumstances, their duties are proactive may intelligence gathering; uncover operations, restrictive operations and surveillance amongst others.

1.4 Research Objectives

The primary objective is to develop an intelligence and security framework to counteract insurance fraud targeted at insurance companies offering services to low-income earners in Zimbabwe. Complementary objectives are to:

- 1) Investigate the causes of insurance fraud in the microinsurance industry in Zimbabwe;
- 2) Evaluate the impact or threat level of insurance fraud targeted at low-income earners to national security and interest;

- 3) Assess the role of security intelligence organisations in countering insurance fraud in the microinsurance sector in Zimbabwe and;
- 4) Prescribe other strategies that can be fused with security intelligence to counter insurance fraud in the microinsurance sector in Zimbabwe.

1.5 Research Questions

- 1) What are the motivators of insurance fraud in the microinsurance sector in Zimbabwe?
- 2) Is insurance fraud targeted at the low-income sector in Zimbabwe a threat to national security and national interest?
- 3) What is the role of a security intelligence organisation in countering insurance fraud in the low-income sector in Zimbabwe?
- 4) What other strategies can be combined with security intelligence to counter insurance fraud in the low-income sector in Zimbabwe?

1.6 Conceptual Framework

In sync with research objectives and questions, this study acknowledges the need to develop an integrated approach that initially illuminates and gives a clear understanding of factors contributing to insurance fraud in the low-income sector of Zimbabwe. Subsequently, research discoveries and recommendations of this study can safely be presented following a religious investigation of variables, determinates or motivators both internal and external that influence micro insurance fraud irrespective of the source of the crime being an individual or an organised group. The conceptual model according to Figure 1.1, the following is proposed. There are internal variables and external variables that are being exploited by organised crime syndicates to peddle insurance fraud in the microinsurance industry, with employees committing the crime in isolation or collaboration with policyholders. Secondly, the reason why organised crime syndicates are targeting micro-insurance service providers is that there are huge cash inflows considering the enormous numbers of policyholders in this market combined with poor internal control systems and investment in technology to counter insurance fraud. Referencing previous studies on fraud, particularly micro insurance fraud investigation frameworks in the non-life insurance business, Lesch and Byars (2008) revealed a significant prevalence of insurance fraud claims attributed to poor handling and detection of these fraudulent insurance claims. Taking into cognisance the daily increase of cases of micro insurance fraud and huge amounts lost daily, a minimum of twenty-five (25) attempts and between ten (10) and thirteen (13) successful cases daily across Zimbabwe (Insurance and

Pension Commission 2022). The penetration rate is alarming and poses a security threat to both national security and the viability of insurance companies. Hence, once a crime is declared a threat to national security, this triggers the deployment of national security intelligence as a countermeasure. However, there is a need for an integrated approach in which a proposed fusion of both security intelligence and internal organisational systems such as internal policies and procedures and artificial intelligence could both strengthen insurance fraud countermeasures.

In investigations and research about insurance fraud, various dependent variables entice an individual to commit insurance fraud. The notion of the equity theory draws from the exchange, departure and social comparison theories in making predictions about managing relations among individuals (Adams, 1963). Equity theory focuses on the effort of input against the expected outcome from an individual's effort. Naturally, employees compare inputs they offer in terms of labour and expertise with outcomes they receive for their efforts and so are policyholders in insurance (Al-Zawahreh, 2015). A disparity between the two is a plausible source of fraud, particularly among employees. Further, an individual's behaviour is determined by their purpose to undertake the behaviour, which is determined by their attitude toward the behaviour and subjective norms, according to the theory of reasoned action (TRA) (Fishbein & Ajzen, 1975). An understanding of why individuals commit fraud is emphasised in the fraud triangle which was developed from preliminary research done by Cressey (1950). Three elements could push an individual to engage in a criminal act of fraud namely non-shareable financial problem, opportunity and rationalisation by the individual who would have identified a fraud opportunity. The first element triggers an individual to commit a crime. However, the pressure or motive to commit a fraudulent act triggers the desire, but does not work in isolation; it is complemented by the other two elements which are perceived opportunity and rationalisation (Cressey, 1971). These elements were adopted in this study where an individual's situation and other external elements compel one to commit insurance fraud.

In light of the foregoing, the conceptual model of this study conceptualises insurance fraud as a highly surreptitious crime which is very difficult to detect, a crime organised and peddled in highly secure and secret circles of organised crime syndicates. Deterrence theory proponents argue that people decide whether to comply or break the law after weighing the opportunity, benefits and consequences of their conduct (Dutton, 1999). Hence micro insurance

companies should deploy four (4) capabilities to counter insurance fraud both emanating internally or externally namely proper internal organisational policies and procedures, security intelligence systems, artificial intelligence systems and internal control systems that will capacitate with capabilities to detect, prevent, sanction, investigate and redress insurance fraud. It is against this background that this study proposed the concept referred to as the CEPSI 360. The acronym CEPSI abbreviates for customers, employees, participation, systems and intelligence which are focus points for insurance fraud elimination and complete insulation of the microinsurance industry.

1.7 Research Design and Methodology

A research design is solely a scientific strategy to investigate a research problem, intending to lay out the procedures for collecting data and analysing it in accordance with the research objectives (Grey, 2014). The objective of the research design is on capturing most useful and accurate data required to address the overall research objectives (Tobi & Kampen, 2018). According to Denzin and Lincoln (2005), the nature of the research question and the issues under investigation determines the research approach or strategy. As a result, an investigation's study style should be viewed as a tool for answering the research question. The study followed a quantitative research design. The design is based on the method of investigating through surveys as a method of data collection, complemented by other techniques such as interviews, document inspection and focus groups as it aims to identify the causes of insurance fraud in the low-income sector. Quantitative approaches can uncover underlying relationships in data that provide a comprehensive understanding of the overall complexities of the situation under investigation (Albers, 2017:15).

1.7.1 Unit of analysis and sampling

This study was carried out in Zimbabwe, covering the twelve provinces of Zimbabwe in which insurance companies and the security intelligence, the President's Department are provincially headquartered. The study used probability sampling with a stratified sampling method, with respondents chosen at random on a proportional basis across twelve provinces. Sampling frame statistics show a population of research participants drawn from regulated micro-insurance service providers and the Zimbabwean intelligence community which comprises the President's Department, Zimbabwe National Army, Military Intelligence Directorate and Zimbabwe Republic Police, Internal Security Intelligence and

Insurance and Pension Commission (IPEC). Based on the Taro Yamane sample size calculation, a sample size of three hundred and twenty-six (326) was determined.

1.7.2 Data collection

Quantitative research depends on surveys as a tool for gathering data (Edmonds & Kennedy, 2017:27). For effective data collection that responded to the research objectives and questions, the researcher maximised on four distinct methods namely survey through a questionnaire, interviews, focus group and document inspection. The questionnaire was the primary data collection tool in this study. It was made up of standardised questions that were asked in a predetermined order to obtain individual data on a variety of problems, primarily and primarily connected to the research objectives, kinds and causes of insurance fraud, threat level, the socio-economic impact of insurance fraud, modus operand used by organised crime syndicates to expand their criminal activities, frequency of insurance fraud cases, measures being implemented in the industry to mitigate insurance fraud, profile effective countermeasures and assess the role of the security intelligence organisation in countering insurance fraud (O’Leary, 2014). The questionnaire was complemented by interviews both face-to-face and telephone interviews which helped in clarifying some grey areas while telephonic interviews are cost effective, efficient and easy to administer, since they can be done irrespective different geographical locations of the interviewer hence reduces potential response bias (Bryman, 2014:214). Further focus groups assisted the researcher to obtain a better grasp of issues under investigation and collect more data in a shorter period, while document inspection gave the researcher insight into historical data of cases of insurance fraud and organised crime syndicates. Further, given the researcher “eyes” only access to personal, sensitive and classified intelligence. Importantly, the researcher selected the methods of research and deployed them in accordance with Coronavirus (COVID-19) research protocols. Coronavirus (COVID-19) restrictions instructed social distancing and non-physical contact interactions hence doing away with face-to-face contact. In that regard, one-line questionnaires, telephonic interviews and virtual (online) focus groups become the most ideal available method of data collection method. Hence on application, this become the most legal, efficient and convenient method in which research participants and the researcher adhered to government restrictions on travel and social distancing interventions to curb the spread of coronavirus (COVID-19).

1.7.3 Data Analysis

Post-data collection, quantitative data was analysed using Structural Equation Modelling. A descriptive analysis was used to summarise the main elements of the data in this study. Summaries with regards to research participants sample and measures were created with the use of visual presentations of pie charts, and graphics analysis. Structural Equation Modelling (SEM) was commonly employed to investigate the causal linkages between latent variables assessing whether the hypothesized structure fits the data well, or in other words, whether there is a relationship between the observed variables and their underlying latent, or unobserved, constructs (Child, 1990). Before conducting the Structural Equation Modelling analysis, the Statistical Package for Social Science (SPSS) analysis was utilised to conduct an in-depth critical analysis by including huge numerical and text data. The data was transferred to the Structural Equation Modelling, for further analysis. The Statistical Package for the Social Science (SPSS) improved the quality of data, authenticity and clarity which all enhanced interpretation and understanding of the interrelationship between the variables under investigation. Cronbach's alpha was also used to assess internal consistency and the link between variables that were closely connected. It is thought to be a scale dependability indication. While the Likert Scales was deployed for analysis because of its advantage of not requiring a simple yes or no response from the respondent, but rather allowing for a range of opinions, including no opinion at all. As a result, quantitative data was acquired, implying that the data may be evaluated very quickly.

1.8 Significance of the Study

The significance of the study is in determining the threat level or degree of the crime of microinsurance fraud. The growing prevalence of microinsurance fraud has created an obvious danger to the operations of stand-alone microinsurance service providers. This has jeopardized both national security and public interest. According to the literature analysis, micro-insurance fraud has hampered investment and closed several revenue inflow channels. Against this backdrop, the primary goal of this research is to examine the numerous causes and sources of microinsurance fraud, the harm they offer, and profile solutions that may be combined with security intelligence. Given the limits of previous research on microinsurance fraud, the purpose of this study was to pave the way for future research on the subject. Creating an intelligence and security framework to combat insurance fraud targeted at

insurance businesses in Zimbabwe that provide services to low-income earners would be beneficial for:

- **Insurance companies:** To understand the nature, current trends, emerging trends and insurance fraud threats to both the company and the state. Inform on internal and external measures to counter insurance fraud. Formulate effective company policies that would eliminate insurance fraud. Invest in proper artificial intelligence, and human capital training as a countermeasure as well as clarify the role of a security intelligence organisation. Short-term and long-term benefits of implementing counter-strategies.
- **Government:** To formulate informed legislation that minimises or eliminates micro insurance fraud. As a proactive measure, deploy security intelligence apparatus to detect and eliminate micro insurance fraud perpetrated by organised crime syndicates.
- **Intelligence and other security organisations:** To increase operational effectiveness (tradecraft). Proactive through target profiling, monitoring of organised crime syndicates, intelligence gathering, electronic surveillance, evidence collection, covert action and influence, and research-based change in policy and legislation.
- **Insurance and pension commission:** To act as an insurance regulatory authority. This study would inform the formulation of policies and strategies to monitor compliance by insurance companies concerning measures and strategies to minimise insurance fraud.

1.9 Scope of the Study and Chapter Outline

This study focuses on all microinsurance companies in Zimbabwe offering microinsurance services to low-income earners. Research participants for this study were selected from various micro-insurance service providers. In addition to the insurance company, the study also targeted the only insurance and pensions regulatory authority in Zimbabwe, the Insurance and Pension Commission (IPEC) as well as the security intelligence community that comprises the President's Department, Zimbabwe National Army, Military Intelligence Directorate and the Zimbabwe Republic Police, Internal Security Intelligence. Employees and officers in the above-mentioned organisations constituted the research population or sample. This study's scope described the extent to

which the research area was explored as well as the parameters used to carry out the study. The microinsurance market mostly serves low-income individuals, and insurance fraud in this sector has become a threat to human and national security. The identified threat would, however, require an extensive study as well as well-coordinated proactive responses and prevention measures. Governments, insurance sector governing bodies, auditors, intelligence officers, and forensic professionals around the world have enormous challenges in detecting, combatting, and preventing insurance fraud in the microinsurance market. Insurance companies are combatting insurance fraud, and have recently made significant investments in artificial intelligence, as well as ironclad internal operational systems and resources, including well-trained human capital (Global Claims Fraud Survey, 2017). The insurance industry's failure to include the security intelligence component is thus a big omission. In light of this exclusion, this study also sought to explore the role of security intelligence in micro insurance fraud detection.

The researcher divided this study into seven chapters to address the study questions. The first chapter presents the problem statement, research objectives and questions, as well as the study's significance. Furthermore, Chapter one (1) of this study spells out how the objectives reflect on the problem statement and determined how the research process. It describes how the planned research would be of benefit to the academic field. This chapter, therefore, helped to inform the reader of the research topic. Chapter two (2) dwelled much on the threat of insurance fraud and the possible role of security intelligence in countering insurance it includes an overview and review of current literature on insurance fraud and, in particular, micro-insurance fraud and the chapter also outlines security intelligence literature. The next section, Chapter three (3) is the theoretical review chapter which intended to theoretically explain the causes of insurance fraud. The fourth (4) chapter explained how the study was conducted. It describes the research technique, that is, the plan used to address and respond to research questions while also addressing research objectives. The research design, population sample, sampling methodologies, data analysis models, and methodology limitations are all covered in this chapter. The analysis component that gave meaning to the data obtained highlighted data display, analysis, and discussion. Pictorial representations and tables were also used to present the findings acquired from the primary data. The research findings are presented in summary statistics. Finally, the fifth chapter contains a

summary, conclusions, and recommendations. Chapter five (5) was the research and data analysis chapter through the deployment of structural equation modelling, and confirmatory factor analysis. While chapter six (6) was an in-depth critical discussion of the research finding in sync with the research questions and objectives. The final chapter, chapter seven (7) was the recommendation chapter. This chapter modelled countermeasures that could be implemented by individual insurance companies and the insurance industry as a whole through a developed concept known as the CEPSI 360 which abbreviates for customers, employees, participation, systems and intelligence which are focus points for insurance fraud elimination while 360 proposes the totality or complete insulation focus of the concept in eliminating insurance fraud.

1.10 Structure of the Thesis

The thesis is structured and divided into (7) seven chapters, each chapter of the seven chapters has its contributory role to the finalisation of this study and also putting checks and balances in terms of addressing the research questions and objectives as outline below:

Chapter One: The first chapter serves as an introduction and background, highlighting the research problem under examination as well as the study's main research aims.

Chapter Two: The second chapter provides an analysis of the microinsurance landscape paying particular attention to types of insurance fraud, insurance legal framework, distribution channels, threats and cost of insurance and an overview of the Zimbabwean insurance industry. Further a dissection of the importance of insurance to low-income earners and the threat posed by micro insurance fraud.

Chapter Three: The third chapter is a theoretical framework that outlines numerous ideas that offer the reasons for insurance fraud as well as countermeasure theories.

Chapter Four: The fourth chapter considers the research design, and scientific strategy to investigate a research problem, intending to lay out the

procedures for collecting data and analysing it following the research objectives.

Chapter Five: The fifth chapter contains the research findings and data analysis utilising descriptive analysis. The conceptual framework is modelled and validated using SEM in this chapter.

Chapter Six: The sixth chapter presents a critical assessment of the study findings concerning the research objectives, as well as an interpretation of the results in comparison to interpretations in the literature review and previous research.

Chapter Seven: Finally, the seventh chapter contains proposals from academic scholars, practitioners, and institutions interested in the subject under consideration. The study's limitations and implications for future research are also examined, and final observations are made about the entire study.

1.11 Chapter Summary

Finally, for research to be relevant, it must have a purpose, which is why the first half of this chapter focuses on the study's goal. The research topic and study objectives were determined, and the remainder of the dissertation was designed to outline the approach to achieving the research objectives. The synchronisation of research objectives, research questions, and the research problem was identified as a significant departure point in mapping out the research process in terms of presenting the conceptual underpinnings of the research, research questions, hypotheses, and fundamental research design. In the introduction, the significance of the study was developed by addressing how it is distinct or different from other studies, how it addresses something unknown or never explored before, or how it expands earlier research on the problem in some way. Chapter one (1) of this study defines keywords utilised throughout the thesis, finishing with a broad framework of the thesis structure. The following section of the study, Chapter two (2), includes a review of the literature pertinent to this study, with a focus on the threat of insurance fraud and the function of security intelligence in combating insurance fraud.

CHAPTER TWO

Threat of Insurance Fraud in the Low Income Sector and Role of Security Intelligence

2.1 Introduction

Insurance fraud in the low income sector is a social and security issue that has become a threat to both human and national security hence requires an integrated and well-coordinated proactive responses and prevention measures. The Southern African Development Community (SADC) alongside the United Nations (UN), the African Union (AU), complemented by governments, the insurance industry governing bodies, auditors, non-governmental organisations (NGOs), civil service organisations (CSOs) and forensic professionals around the world, are facing numerous challenges to detect, counter and or contain insurance fraud particularly insurance fraud perpetrated by organised crime syndicates who have since targeted insurance service providers offering services to low income earners. Recent studies by the Insurance and Pension Commission (2020), following realisation by insurance companies that insurance fraud had increasingly become a threat to the survival of micro insurance, insurance companies have since started to pour significant investment into artificial technology combined with watertight internal operational systems, and resources such as well-trained human capital to detect and counter insurance fraud.

It is important to note that insurance fraud is a highly surreptitious crime. The threat of insurance fraud is also stretching to national security with a possibility of regional destabilisation in Southern Africa. The surreptitious nature and threat levels increased as organised crime groups' access commercially available technology that allows them to exploit weaknesses in insurance companies offering services to low-income earners (Zimbabwe Republic Police, 2018). Preliminary research done so far by the Economic Crime Institute (2003) suggested that insurance fraud is increasingly becoming a global threat to national security, citizens, the economy and global commerce as it facilitates a wide range of organised crime activities and terrorism hence compromising human security. Localised and transnational organised crime syndicates operating nationally, regionally and at a global level benefit from differences and lack of internal counter measures in micro insurance service providers. In addition, some organised crime syndicates operating from developed economies such as Britain, Unites States of America and Australia amongst others have access to advanced technology hence exploit the weakness of lack of technology amongst African

based micro insurance service providers. The technology over years has been exported to African based organised crime syndicates groups hence take advantage of micro insurance companies that cannot afford counter insurance fraud technology particularly those operating in less economically developed economies in Africa. Lack of national enforced countermeasures such as deterrent policies and legislation, non-participant of security intelligence in countering insurance fraud and lack of policyholders' awareness, especially in African based insurance companies, have been enabling factors for most types of insurance fraud (Insurance and Pension Commission, 2018). This chapter presents material relevant to the study's objectives with the goal of gaining an understanding of the broad overview of Zimbabwe's insurance market. The literature review clarified on what is insurance, micro insurance, insurance fraud, types of insurance fraud, the cost, and the hazards of insurance fraud. Further, the chapter gave a review of how low-income earners are being affected by insurance fraud, why organised crime syndicates target insurance companies offering services to low-income earners, as well as ascertain the role of a security intelligence organisation in countering insurance fraud. Most importantly, the literature discusses the theoretical, conceptual and empirical review, dissecting the anatomy of micro insurance fraud.

2.2 What is Insurance?

Insurance has contributed significantly to societal economic growth by ensuring the smooth operation of the risk management processes. The insurance industry developed financial institutions and reduced uncertainty by strengthening financial resources available to individuals and corporations, which has been extended to low-income earners and households in the form of micro insurance. The Insurance and Pension Commission (IPEC) (2020), Zimbabwe's insurance and pension regulatory agency, affirmed that the prospects of loss generate uncertainty and has a negative economic and psychological impact, particularly among low-income earners. A lack of risk containment capabilities is a more direct indicator of a state's human security vulnerability. Low-income earners are disproportionately affected by such risks and losses because they lack established safety nets, and governments are having difficulties in providing such necessary social security to this segment of the economic sector.

Insurance is crucial to all citizens around the world, regardless of individual and household income levels or economic sectors. In this perspective, insurance is the single most essential and extensively used risk management option for most people, families, and businesses.

Individuals all across the world, regardless of income or economic sector, desire security. Second from food, clothing and shelter, insurance in the modern world is highly desired safety net that secures the insured, policy holders in diverse ways, hence security brought about by insurance is suggested to be the most important goal or desire an individual would want to achieve (Kanengoni, 2020). In conformity, insurance is an alternative form of human security, excluding that given by security personnel (Insurance and Pension Commission, 2020).

It is critical to comprehend what insurance is, its evolution, and its significance in society and the state. Various academic and insurance industry definitions of insurance exist. According to Outreville (1998), the consensus between the two parties brings about the insurance contract. In the insurance contract, the insurer, insurance company agrees to pay an amount, possibly once of payment to the policyholder or a third party, in exchange for a premium or an assessment, once the insured risk event takes place. It is frequently referred to as an indemnification agreement or contract. It is assumed that the insured will not profit from the insurance and will only be compensated to the degree of financial loss. However, organised crime syndicates are in some cases exploiting insurance companies for personal financial benefit. The Criminal Investigation Department (2018) which is the Zimbabwe Republic Police department that is tasked with criminal investigations highlighted that organised crime groups desire for easy access to unjustified financial benefit. In that regard they target insurance companies offering services to low income earners due to poor internal security, policies and procedures. This attributed to the rise of insurance fraud crimes cases in Zimbabwe.

Despite the fact that various definitions have been proposed from different backgrounds, the academia, professional bodies and institutions, legal and insurance experts agreed that one of the most helpful and widely recommended definitions of insurance fraud is to define insurance as a mechanism, a safety net, or a service that transfers identified risks of financial loss to an insurance company in turn, the policy holder is expected to pay premiums, as service to the insurance contract. The need to pay a premium to the insurance company is stipulated in the insurance contract and paid at agreed intervals; insurance companies function as financial intermediaries, investing the premiums they receive to offer this service. The net premiums issued, or premium revenues less reinsurance expenses, are commonly used to determine the size of an insurance firm. The three most common insurance industries which

appeal to the low income sector are insurance for property and casualty, life, and health insurance.

Insurance, according to Dror (2018), is a comprehensive risk management financial instrument based on the idea that anything of monetary value is worth preserving by passing the risk of loss or damage to someone else who agrees to pay compensation. Accepting to insure a prospective policyholder is known as insurance underwriting in insurance law. Insurance underwriting necessitates complicated estimates of the reasonable price or insurance pricing of the specific risk being transferred from the policy holder to the insurance company. The value proposition of insurance is a concise statement that describes how the insurance contract, policy solves or improves the condition of consumers through the quantified value of specific benefits payable to them. Insurance Europe (2018) stated that insurance is designed to guard against substantial but unpredictable losses by pooling risk. This pooling mechanism is harmed by insurance fraud because insurance fraud depletes money secured by honest policy holders in anticipation of risks as well as incapacitating the ability pay for such legitimate losses. The insurance system entails risk management, risk transfer and mitigation and is based on a shared responsibility principle between the insurance company and the policy holder. In that regard, all forms of insurance fraud compromised this position hence posing a threat to the policy holder, the insurance company and the state.

An understanding of the insurance mechanism is important particularly amongst low income earners. Communication is critical in the adoption of insurance services and products, both parties should understand and concert to terms of reference in the insurance contact according to the IPEC (2020). Over years' insurance companies have developed various advertisements which are being communicated via diversified channels with social media particularly WhatsApp in Zimbabwe taking a lead followed by television and print media, respectively. Insurance companies operating solely and the insurance industry's insufficient or non-existent of well-established communication channels with potential policyholders has largely contributed to a lack of knowledge of the importance of insurance to society and a barrier to selling insurance products and services to low-income consumers. The IPEC (2019) confirmed that individuals in the informal light industries in Harare the capital of Zimbabwe are not even aware of micro insurance services even within their areas of jurisdiction. Communication is crucial, lack of it has accounted why a significant number of forty per cent

of low-income earners in the informal light industry do not have any form of insurance to cover for the simplest risk such as health and or funeral typically in Zimbabwe while this arrangement or organised insurance mechanism is therefore an important safety net.

Insurance, society, and social behaviour are all dependent variables on the insurance system. In its most basic form, insurance relieved individuals and institutions of the financial burden of unexpected misfortune and loss by providing compensation or after risk services. Insurance have provided the most needed services such as the support of a family for instance if the breadwinner passes on, also in dire health situations medical aid encourage people to seek medical assistance without fear of financial ruin, re-establishing confidence amongst policy holders through the aid to a homeowner or company owner in rebuilding, reestablishment of business and or property after a fire or destruction by natural phenomena, and protect both customers and producers from a defective product. Individuals or entities who are categorically designated as policyholders are involved in the insurance process at its most basic and fundamental level. The policyholder agrees to pay a set amount, on a regular basis or at regular intervals into a common fund or insurance system, usually monthly premiums. Money is drawn as pay out for a claim to reimburse one or more policyholders who are victims of a predefined occurrence under specific parameters or extent of coverage in the event of a risk that demands intervention.

As a result, the insurance policy and agreement between two parties that is the insurer and insured, a contract built on mutual trust and understanding. It is a partnership in which the policy holder preferred to pay a fixed sum on a regular basis to be protected against an unpredictable loss, the financial repercussions of which would be catastrophic and much higher in the absence of insurance cover. Risk, or rather, "shared risk," is an important phrase in insurance or the insurance contract. The chances of the insured event occurring and the repercussions effect both the insurance company and the policyholder, although not in the same way. Furthermore, the risks associated with an occurrence are comprised of considerably more factors than just recurrent chances. In the case of accident insurance, factors such as age, environment, lifestyle, and behaviour all influence not just the likelihood of an accident but also the size of the loss if one occurs. All parts of the insured risk must be adequately assessed, or "actuarially estimated," for the arrangement to be fair for both parties and the premiums paid by the policyholder to accurately reflect the risk insured. This should overly consider the breadth and specific nature of the occurrence, the extent of the benefits

paid, the policy holder characteristics, and number of individuals or entities covered for a similar risk at the same time, a concept known as risk pooling or sharing. To put it another way, premium pricing and risk assessment are not random decisions made solely at the discretion of insurers. This concept of "shared risk" between individuals and insurers is significant because it emphasizes the ideals of solidarity and individual responsibility that have long been central to the insurance mechanism. Indeed, the aspect of insurance solidarity cannot be perpetuated unless each individual member of the insurance pool takes responsibility for risk prevention and mitigation.

Insurance in its pure form is an acceptable cost-effective safety net and a social good. Its application to low income earners is viewed by government as noble since it eases pressure on government to provide social safety net (National Social Security Authority, 2021). In some spheres and economic sectors, insurance is classified as a public good. Individuals and businesses can use insurance companies, mutual funds, and cooperatives to protect themselves against rare but severe losses at a low cost compared to the predicted loss. They accomplished so by using the central limit theorem and the law of large numbers, which guarantee that a big enough number of basically homogeneous risks will give well-behaved and highly predictable aggregate results based on a roughly Gaussian loss distribution. Global insurance spending was estimated at a total of four thousand six hundred and thirteen billion United States Dollars in 2012. Modern life would have been impossible without this form of risk management, hence in that regard, insurance companies are offering social security nets that are being applied by individuals as risk mitigation measures.

2.2.1 Micro Insurance

Countless research by various insurance professionals have been forwarded in response to the depressing circumstances of the many millions of low-income earners who are labelled marginalised, primarily in Africa's less economically developed countries, Zimbabwe included. When considering the possible role of insurance mechanisms, particularly micro insurance services that can be extended to low-income earners, it is critical to have a thorough awareness of the conditions and risks low-income earners and their households face. According to Patel (2002), the informal sector accounted for between fifty and sixty percent of the workforce in most less economically developed African countries. It can reach ninety percent in extreme cases, given that most people in Africa begin working at the age of ten (10) for males and twelve (12) for female (Zimbabwe Statistical Agency, 2019). The

informal sector is characterised by relatively tiny, family-owned businesses that cater to limited local markets with little capital investment and low labour intensive skills. The number increases with polygamous families particularly those who depend on farming. In some cases, small entities that are partially doing well in their small enterprises employ individuals as additional labour. However, workers in the informal sector lacked official employment contracts, unaware of their rights, and not represented by any effective labour unions. Furthermore, because of the lack of legal financial institutions, rogue moneylenders have taken advantage of the impoverished through informal savings schemes (Ford Foundation, 2000). In that context, micro insurance was regarded as a panacea to counter the risk faced by low-income earners in less economically developed African countries.

A 2021 study conducted by the Zimbabwe Public Service Commission, which handles government human resources management issues from recruitment to compensation, indicated that the definition of low-income earners should not just be limited to workforce in the informal sector, but should be inclusive of the government and private sectors. The report categorically stated that low-income earners in Zimbabwe are measured by the level of income per household, with a unique situation that showed individuals in the informal sector may generate more income as compared to those formally employed in the various formal sectors. The IPEC Director Machinjika (2019) contended that there was a notable increase of voluntary exclusion of employees formally employed in the various formal sectors from insurance services due to increases in premiums which eroded their net salaries. A study by the Zimbabwe Statistics Agency (2020) showed that eighty-six per cent of formally employed employees in Zimbabwe found insurance highly expensive and unaffordable hence these individuals fall in the category of low-income earners.

In that regard, the definition of micro insurance has been broken down into two parts. The first part was to define what insurance is, and the second was to define what micro insurance is? The IAIS (2018) defined micro insurance as "protection of low-income persons against specific risks in exchange for recurrent premium payments according to the risk likelihood and cost." According to IAIS, insurance provides a trade-off between an unaffordable or severe loss that is unclear and an affordable loss that is certain, i.e. the premium paid at agreed intervals. The potential market for insurance in developing economies is anticipated to be between one point five and three billion policies, according to Lloyd's 360 risk insight (2019). A wide range of insurance products are in high demand

particularly in the micro insurance industry and these may include health and life insurance, agriculture and property insurance, and disaster insurance. With operations in over two hundred countries and territories, Lloyd's of London is the world's largest specialty in micro insurance market. It is typically the first to insure risks that are original, distinctive, or difficult to insure. Insurance solutions for low income earners and households are not a new notion in the global insurance sector. Industrial insurance in the nineteenth and early twentieth centuries was the forerunner of today's micro insurance. Despite this, insurers are yet to cover most low-income markets in the developing world. Fewer than five per cent of low-income people have access to insurance, and even fewer have access to the items they require.

According to Dror (2014), there were several approaches have been applied to define, explain, and understand what insurance meant for low income earners. Professionals in the insurance industry alternatively have termed insurance for low income earners micro insurance. To begin, microinsurance can be defined as a feature of the financial status of low-income policyholders in emerging economies. Second, micro insurance can be defined as a set of products and services in which an insurance firm provides limited benefits in exchange for tiny premiums. Finally, micro might be thought of as a property of the process of creating and administering the schemes. Micro insurance, according to Churchill (2006), is insurance meant for low-income earners, insurance against specific, specified risks in exchange for premium payments equal to the risk's chance and cost. Dror (2014), on the other hand, wondered how impoverished one should be in order for insurance coverage to be called micro. This argument varied by country and insurance company, but in general, micro insurance is for people who are not covered by mainstream commercial or social insurance, and who have not had access to proper insurance products. Micro insurance is of particular relevance because it provided coverage to people employed in the informal sector, without access to commercial insurance or social employee-employer social safety nets which comes with the employment contract or indirectly issued by the government. Other personnel in the government and well-established private sectors are likewise considered low-income earners by virtue of their job grade and salary, according to the Insurance and Pension Commission (2019). Dror (2014) despite the fact that the definitions differ in their approaches to micro insurance, they all share four essential common, overlapping aspects, which included:

- Insurance meant for low income earners employs risk pooling principles;
- Micro insurance is designed for low-income individuals;
- Micro insurance is aimed for persons who work in the informal economy and;
- Micro insurance is not affected by the type of risk, such as life, health, agriculture, livestock, or assets.

Micro insurance has been viewed from a different perspective by various stakeholders. Commercial insurers view micro insurance as a method to access enormous underserved customers, primarily low-income individuals, even in the most remote locations. Development oriented organisations such as the African Union, the World Bank, and the United Nations has since placed micro insurance as a strategic initiative with capabilities that has assured poverty reduction by providing social safety nets that complement human security endeavours. According to academics, finance sector expansion has been important as industrialisation for long-term economic success. Micro insurance has served the same function as regular insurance in that it allowed users, whether individuals or businesses, to transfer risks and obtain the security they required to live their lives or build their businesses. Micro insurance, with its promise of profitability and welfare advantages in markets with billions of clients, deserved to be included in both business and development initiatives. For numerous reasons, micro insurance could be a critical new risk management instrument for Zimbabwe's low-income earners. Vulnerability has a significant impact on impoverished people in a variety of ways, reinforcing or exacerbating their poverty. According to Zimbabwe's Minister of Mines and Mining Development, Chitando (2019), artisanal miners in the Mazowe and Midlands districts, for example, are concentrated in a small area and hence suffer from greater rates of malnutrition, leaving them more vulnerable to illness, injury, and death. They lack the necessary information and financial resources to make informed preventative or reactive decisions, and they commonly hold beliefs that exacerbate their conditions when dangers such as the death of the household's breadwinner arise. Furthermore, they are usually unable to deal adversity owing to the lack of regular solutions such as medical care insurance and funeral coverage, which are frequently unavailable.

Micro is characterised by the target market, specifically the low-income earners, according to the South African Insurance Industry Survey (2017), poorer people, especially those with low-incomes, are often shut out of the official financial services market since they are

regarded poor and incapable. The fact that they are not technically working exacerbated the situation because they do not have access to these benefits through employment, where the employer can pay a set percentage of the premium. As a result, micro insurance provided them with access to the formal insurance market by producing bespoke products and distribution methods that were adapted to their individual requirements. Given that low-income earners in largely less economically developed third-world countries are the targeted market group for micro insurance, it is in the providers' best interests to maintain their goods, plans, and services as simple and cost effective as possible. The target market for micro insurance is a guarded and basic one. It is however difficult to build a market for something as unique as micro insurance worse if the targeted consumers realise it takes too much work to understand and does not deliver good value for money. Second, the distribution channels that appealed to the city, modern and educated market group was not acceptable or compatible with rural residents, particularly low-income earners. In this context, developing strategic collaborations for effective creative distribution channels was prudent.

Commercial insurers targeting low income earners engaged mobile phone network operators and government development agencies to truly expand the reach of micro insurance services. The development of an insurance culture among low-income earners was necessary. Not every low income earner had accepted or trusted insurance. This is why grassroots efforts to raise knowledge of the product's usefulness and benefits were so important. Collaboration with other businesses, service providers and the government to develop a deeper grasp of the market landscape could have resulted in more efficient solutions. According to recent estimates, the developing world has around five hundred million individual low income earners who are seriously considering micro insurance services, with the number expected to rise to one billion by the end of the decade (Micro Insurance Network, 2013). Governments, insurance companies, and providers all across the world have since stepped up their efforts to expand the geographic reach and range of insurance services offered to low-income earners. Emerging countries have since abandoned desktop computers in favour of mobile phones, which are multi factional communication tools, according to current technological trends. A remarkable percentage of African population including low income earners currently use a mobile phone, and approximately a quarter utilises the internet on a regular basis, as fixed telephone lines have become increasingly scarce and to some extent outdated. The percentages of adults who own a smartphone and regularly use the internet have increased

dramatically in the last two years, according to a Pew Research Centre (2017) survey. Despite these improvements, only about five per cent of low-income earners have access to the insurance or coverage they need, making developing countries a lucrative market to tap into, a market that can easily be accessed via mobile phones.

Micro insurance through mobile phones or mobile phones network operators is a novel manner of distributing insurance services in developing nations. It is not merely a low-cost coverage for the poor. With an average annual growth rate of ten per cent micro insurance has covered around one hundred and thirty-five million individuals, accounting for around five per cent of the total market potential. The micro insurance solutions however addressed the basic risks found in the traditional insurance services such as life insurance, property, life, health accidental and disability insurance. Agriculture and farming are the mainstays of developing countries' economies. Moreover, they could not meet all of the needs of an expanding population alone through the things they produce. Around seventy per cent of the world's populations of seven billion people live in poverty. In such a situation, variety of insurance products, including life and health care insurance, agriculture related insurance, disaster and property insurance are in high demand in developing economies (Silvello, 2017). Insurance targeted at low income earners is a cross industry potential for insurance companies to reach closer to their customers by providing the appropriate coverage at the appropriate moment. Connected insurance is the next big innovative idea in the insurance industry. Artificial intelligence, the Internet of Things (IoT), and big data containment will play a role in this innovative initiative. Health, funeral, home, and vehicle insurance are the pillars of this interwoven, dynamic technological ecosystem. This then created opportunities for insurance companies to provide customer centric insurance services while simultaneously bridging the protection gap. In light of this opportunity, the ultimate objective was to reach and engage low-income earners in an efficient and reliable way while connecting their risks with the insurance companies through the use of technology. Existing distribution channels were also being utilised to supplement this technological initiative. Community based groups, mobile phones and network operators and microfinance institutions were the most common distribution channels. However, some insurers continued to sell their products through traditional channels, but this trend is diminishing in Zimbabwe, South Africa, and Kenya, while new channels such as retailer merchants are being explored more. An observed advantage from the technologically related micro insurance pilot programs, institutional

structures have benefits and drawbacks, according to Insurance News around the World (2010). As a result, collaboration between different types of institutions may be a win-win situation. Prashad and Hoffarth (2014), the distribution route was a significant factor for institutions intending to provide insurance to low-income earners. With restricted profit margins, insurers should have identified low-cost alternatives to serve the enormous number of lowly paid customers. Basically, insurance businesses can supplement mobile phone network operators by riding on financial institutions, community-based institutions, retail outlets, employers, and other connected institutions such as healthcare service providers.

Research from various health faculties and institutions exhibited that having health insurance encourages consumers to seek medical attention sooner and more frequently (Dalal et al., 2014; Zimmerman, et al., 2013). This gave healthcare providers an incentive to distribute insurance. Protect, for example, has provided value-added services in the form of a benefit card that saved Peruvians money on healthcare and medication. If healthcare providers are directly reimbursed by the insurer, insurance can help reduce uncollectible invoices. When health care insurance is supplied through health institutions such as clinics, hospitals and pharmacies, the likelihood of adverse selection is apparently larger. Although additional research on the prevalence of adverse selection and the effectiveness of these techniques is needed, waiting periods and enrolling complete families can help. Cooperatives, trade unions, and faith-based organizations are examples of community-based organizations. These organizations have a long history of offering insurance to its members. They vary in size and formality, but their capacity to bring huge groups of people together, sometimes with the same features or demands, makes them all great distribution channels. Many post offices in Zimbabwe are functional and have a long history of providing financial services, and they usually have large client bases, despite the fact that they have faced increasing competition in recent years. Insurance can assist post offices in increasing their revenue and gaining a competitive advantage. The Moroccan post office, for example, has benefited from insurance distribution in terms of customer retention and profitability (El-Moussaoui, 2013).

Employers may also be a source of insurance distribution. Employers who are concerned about their employees' health and who recover quickly after falling ill, for example, will gain. As a result, employers have become an alternative insurance distribution channel as well as a source of insurance subsidies. Products such as voluntary and required products, as well as life and health products, are regularly sold. Supermarkets, appliance stores, clothes retailers,

agricultural input dealers, and credit retail chains are all present in many emerging markets. They frequently sell things that are already on the shelf. Micro insurance in Africa began as a kind of charity pushed by organised groups at the community level, before being formally incorporated into global financial aid programs for low-income earners. As a result, a growing number of service providers have begun to sell cost-effective insurance products to a niche market, low-income earners. Private insurers, mutual insurance firms and funds, microfinance institutions, non-governmental organizations, governments, and semi-public enterprises are among the participants (Mounaji, 2020).

Undoubtedly, micro insurance for low-income earners in Africa has been successful due to two key elements. In comparison to traditional insurance, microfinance services and practices have had a remarkable success in meeting the basic insurance requirements of low-income earners. Secondly, the insurance gap between the perceived wealthy and the poor, low-income earners necessitated the development of creative, tailor-made insurance products to cover risks that were previously uninsurable. These serve as a springboard for micro insurance initiatives that are specifically tailored to provide micro insurance services and programs. Credit life and life insurance were the first micro insurance products introduced in Africa. The dominance of life and credit life insurance was due to the products' profitability for stakeholders as well as the products' distribution flexibility, as they were typically coupled with health and accident insurance policies. Funeral insurance products accounted for seventeen per cent of total premiums collected in Africa in 2017, with countries in the south of Africa such as Zambia, Namibia, South Africa, Malawi, and Zimbabwe being particularly popular. These policies can also be included in a life insurance package. Another popular micro insurance product which was highly accepted by low income earners since its inception is health cover. Over years, the product penetration rate increased dramatically and remarkably in the African market. Health cover has been and it being offered in two ways, by supporting public coverage programs or by directly delivering complementary health products like hospital cash and health value-added coverage. Crop and livestock insurance are often praised and accepted by community farmers and commercial farmers as well, particularly those farming high value or strategic crops such as tobacco, wheat and sugarcane. The product continues to expand as one of the widely accepted micro insurance service, product, with government plans frequently supporting it in Zimbabwe. These programs not only assisted the disadvantaged population who required micro agricultural insurance, but

they also assisted private insurers in dealing with increasing claim rates and cost structures as a result of distribution issues and climate concerns.

According to McCord, Phily, and Harms (2009), low-income earners in Africa have had access to micro insurance in various forms for a long time. Since the 1970s, community-based, cooperative insurers and religious-based insurance have served the African market. The Bamako Initiative paved the way for community-based health insurance plans in the 1980s, particularly in West Africa. Commercial insurers began to enter the market in the mid-1990s, offering specialised micro insurance products. For decades, informal micro insurance has been provided in a variety of forms, ranging from West African "tontines" to East African "friend in need" groups to South African and Zimbabwean burial societies. Over the last ten years, insurance has developed into a widely recognised financial intervention to help Africa's low-income earners to manage their financial risks. According to a study conducted by the International Labour Organisation (2009), fourteen point seven million people, or about two point six per cent of the population lived on less than two USA dollars per day in thirty-two African countries that have already established micro insurance services. Funeral insurance is the most widespread and well accepted micro insurance service in these countries, with coverage extending to even the most distant and marginalised communities. This equates to eight and a half million people, or fifty-six per cent (56%) of the total population. Additionally, out of the total of fourteen and a half million, ten and a half million are covered by products other than credit life. In 2008, regulated insurers collected eighty-eight per cent of the total micro insurance premiums received, totalling two hundred and fifty-seven million United States of America dollars.

McCord, Phily, and Harms (2009) concluded that life insurance products continue to dominate Africa, according to the International Labour Organisation (2019) study in Africa. Credit life covers around nine point five per cent of their potential markets, whereas other life products cover a little more than three per cent. Health services and products, which are frequently regarded as the most in need, only cover roughly zero point three per cent of the low-income earners population, while property and agriculture cover far fewer people about zero point two per cent of the potential market, respectively. It is apparent that Africa still has a lot of room for micro insurance expansion and growth. In some countries, such as Kenya, Namibia, Senegal, and Cameroon, a variety of micro insurance services and products are available, whilst in others, one product line dominates. "Insurers" are described as institutions

that handle insurance risk in such areas. Regulated insurance companies, such as commercial insurance companies, cooperative or mutual insurance companies, health mutual, community-based micro insurance programs, microfinance institutions (MFIs), non-governmental organisations (NGOs), hospitals, and others that manage their own unregulated insurance programs.

About two million low-income earners have confirmed that they have subscribed to various micro-insurance products being offered, largely due to their affordability, following the launch of the micro insurance framework that is in line with the national financial inclusion agenda targeting previously excluded population such as small-to-medium enterprises, peasant farmers, vendors, and other low-income earners (IPEC, 2019). The policy framework called for the creation of micro-insurance products that were affordable to those with the smallest incomes. In this line, various companies created such products with minimum rates as low as USA fifty cents (US 0.50) and pay-outs as high as USA, five hundred dollars (US 500). These items have mostly been distributed as mobile products, with numerous companies additionally providing after sales services via mobile phone platforms. Seventy per cent of adults in the country were uninsured, according to a FinScope poll conducted in 2014. With technology, the thirty percent manage to have insurance mostly funeral insurance, indicating a significant gap in insurance uptake. Zimbabwe's insurance penetration rate was predicted to rise to twenty per cent in 2019 from the current three point six per cent in the following two years, owing mostly to micro insurance.

Insurance companies, mobile phones network operators, and technical service providers have all launched innovative new products in hitherto untapped regions in recent years, propelling mobile micro insurance to new heights. While mobile insurance solutions promised scale, cheaper distribution costs, and associated benefits for insurers and mobile operators, as well as acting as first-level enablers of financial inclusion, many efforts are yet to achieve their full potential. They confronted hurdles such as limited consumer experience and knowledge of insurance, complex and expensive products, a lack of supporting regulation, intricate relationships, and reliance on mobile money in underdeveloped areas. Nonetheless, a number of mobile insurance efforts have broken through these restrictions, bringing affordable insurance to millions of low-income earners. Mobile phones network operators in Zimbabwe such as Econet Zimbabwe Telecel and Net One have huge customer bases and a strong brand; models in which they give their brand and strategic support to the effort have been more

effective. Mobile penetration is predicted to be greater than sixty per cent in sub-Saharan Africa alone. Customers are already engaged with the mobile phone network products, hence this has allowed simplified registration, administration, and claims processing processes in case of insurance. Customers, policy holders have been enrolled via SMS in many situations, eliminating the need to visit an insurance agent.

Further, policy holders were automatically registered based on current mobile phone network operator's data, without having to supply any additional information in some situations. Providing high-quality insurance products ensured growth, particularly in regions where the insurance culture was still growing. Quality products and services were designed to meet low income consumer needs while they were charged reasonable prices, provided easy access to services, simplified product experience and developed a culture of quickly, readily, and honestly fulfilling claims. Low income customers have grown in numbers as a result of the product variety. Auto-enrolling segments of customers that reach specified mobile airtime or mobile money criteria, as seen in programs in Zimbabwe and Zambia, as well as a number of other markets, have helped to improve loyalty models develop quickly and operate as a market maker. The payment system should be market-based when migrating from a free to a premium insurance plan. Because mobile money and debit orders only reached a small portion of the market, relying only on them limited adoption and increased lapse rates. Although airtime is generally available in most places and can be used to collect premium payments such the funeral Ecosure package being distributed by Econet Zimbabwe, the costs of airtime are typically greater than the costs of mobile money. Trade-offs must be considered when developing such products. Multiple channels, such as SMS, USSD, agents, and call centres, were targeted to certain target demographics, which allowed for increased access and increased insurance product sales. Mobile channels helped with adoption, but they often needed to be combined with high-touch (human) models. Despite insurers' and cell operators' best efforts, market regulation can often make or kill a mobile insurance endeavours. Regulators must strike a balance between allowing for innovation and preserving the market. Mobile operators, insurers, regulators, and other industry actors may better handle the challenges these products encounter and extend this important insurance to unprotected and underserved clients by taking these lessons into mind.

According to Dror and Piesse (2014), the three guiding concepts of outreach, sustainability, and offering benefits to all were at the heart of the micro insurance sector's success. A

combination of policy, technology, and risk management was essential to reach these milestones and boost the penetration rate. When a market and demand were discovered, distribution variety was one of the most important components in achieving success. Micro insurance has successfully penetrated and expanded into the middle class in South America, across Columbia, Mexico, Peru, Guatemala, and Bolivia, which over years deployed a wide range of retail distribution channels and with special reference to Brazil, micro insurance was dispatched via and or with mobile network operators and gained significant attention. The rapid growth of micro insurance in African and Asian markets provided a potential to grow inclusive insurance markets. However, there was one dramatic failure in Zimbabwe when EcoLife micro insurance service that was offered and distributed by a leading mobile phones network operator Econet Zimbabwe collapsed. A fifth, twenty per cent of the adult population was impacted overnight due to the immediate cancellation of the product.

There was a desire to encourage innovative, secure new delivery mechanisms to increase access to insurance on one hand, whereas on the other there was the imperative of maintaining trust and stability. A recent study by Micro Insurance Network (2020) estimated that over two hundred and eighty million people are insured by at least one micro insurance policy worldwide. This is great, but it still only accounts for a small portion of the estimated potential market of four billion low-income earners in Africa who are in need of insurance. Reinsurance Group of America (2021) versed that reaching low-income earners might be difficult since some live in the most remote rural regions. These impediments necessitated innovation, however, notably in product distribution and administration. In order to gain economies of scale and lower acquisition costs, insurers must engage with aggregators or channels with a broad presence.

To grasp where micro insurance is going and how it may help bridge the protection gap, there is a need to first understand its history, including both successes and failures. Figure 2.1 below shows that micro insurance has gone through three stages, each of which taught something new about reaching low-income earners and other underinsured customers.

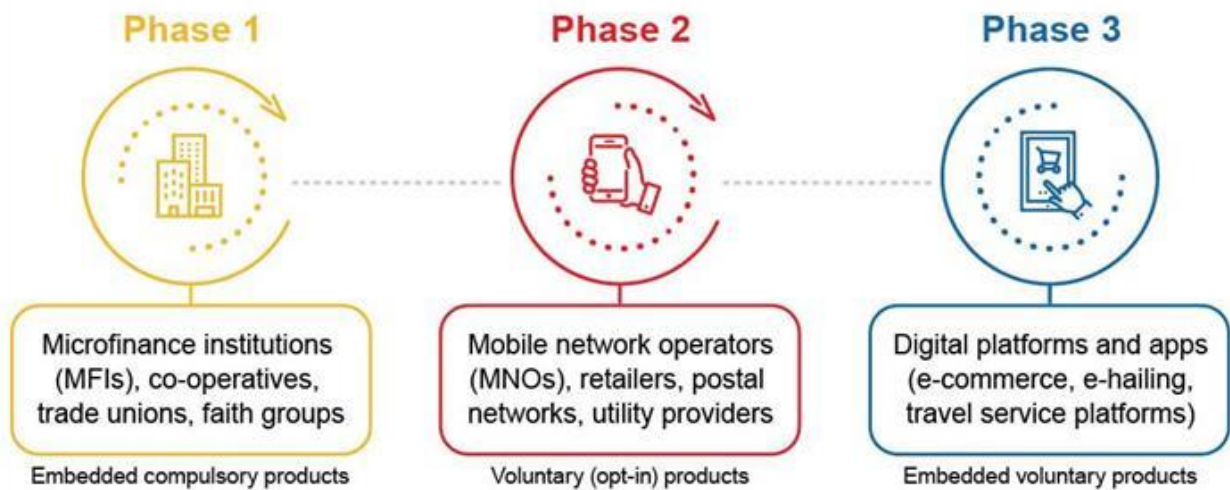


Figure 2.1: Phases of micro insurance distribution

Source: Reinsurance Group of America 2021

2.3 Definition of Insurance Fraud

Globally, various definitions of insurance fraud exist in the insurance industry. In Zimbabwe, the Insurance and Pension Commission (2019) defined insurance fraud as an act that involves a policyholder or a third party in a claims process, in which either party consciously provides wrong or false information or misrepresents material facts during the claims process to swindle the insurance company of money or any benefits which they are not entitled to. Derrig (2002) insurance fraud is a criminal act in which perpetrators illegally or through misrepresentation of material facts obtain financial gain from either or both policyholders or insurance companies. The Insurance handbook (2018) stated that insurance fraud is an illegal attempt by policyholders and their accomplices to either financially or materially benefit from an insurance company by contravening the terms and conditions of the insurance agreement.

The security sector across the globe has contributed to the definition and perception of insurance fraud. In the United States of America, Federal Bureau of Investigation (FBI) (2018), defined insurance fraud as an act of illegally obtaining money, benefit, service or valuables from the insurer or insured through misrepresentation of material facts. The Central Intelligence Agency (2019) further explained that insurance fraud is when a policyholder issues a false statement to the insurer for financial gain. The British Military Intelligence Five (MI5) and Military Intelligence Six (MI6) (2017) both concurred that insurance fraud is a

form of a moral hazard that involves the manipulation of information to unduly benefit from insurance protection. Russia's Federal Security Service (2019) explained that insurance fraud is when a policyholder claims from the insurance company something that the insurer is not liable for. The Zimbabwean intelligence community (2018), which comprises all the security sectors involved in secret services, agreed that insurance fraud is a clandestine criminal act involving criminals who intend to illegally gain money from insurance companies or insured individuals for personal gain and financing criminal activities. In this regard, the International Association of Insurance Supervisors (2007) defined insurance fraud as an act by the policyholder or accomplices to illegally gain dishonest advantage through asset misappropriation, internal organised trading, conscious misrepresentation of facts, suppression or non-disclosure of one or more material facts relevant to a financial decision or transaction, and abuse of authority. The Zimbabwe Criminal Procedure and Evidence Act, Chapter 9 (2017) based on numerous definitions, listed four factors that make insurance fraud a criminal act:

- 1) The act should be organised by two or more people, with a possibility of one person particularly an employee or policy holder also action in isolation;
- 2) Parties involved should “knowingly and wilfully” act to defraud or deceive an insurance company;
- 3) Making a false or misleading statement to an insurance company or intermediaries that hides, avoids relevant information of material facts, or contains falsified or misleading information about any fact material to an application for issuance of a policy or a claim for payment or other benefits under such a policy by conspiring, assisting, soliciting, or conspiring with an accomplice and
- 4) An insurer or any of its agents assisting, conspiring with, or encouraging another person to conduct any act or omission by deception, misrepresentation, or other fraudulent methods.

2.4 Organised Crime Syndicates and Insurance Fraud

A persistent criminal activity known as organised crime involves two or more individuals conspiring to commit a crime. Organised crime syndicates have worked logically to profit from illegal activities that frequently resulted in substantial financial gains (Zimbabwe Republic Police, 2020). Its continued existence and success is based on support by corrupt

political elements within a system, public official corruption and use of advanced technology, the use of intimidation, threats, and security forces to defend operations. Criminal activities peddled by organised crime syndicates differs across countries, locations, crime kinds, and the nature of hierarchical structures, hence a broad definition of organised crime syndicates has limitations. As a result, while knowing the broad characteristics of organised crime syndicates is crucial, understanding how these criminal gangs emerged in diverse locales and criminal settings required more expertise, expertise by security intelligence personnel or agencies who have provided a better understanding of these criminal gangs. The United Nations Convention against Transnational Organised Crime (2003) advised its member states to consider the meaning of organised crime in setting the stage for international action. However, there was no accepted meaning or definition of either transnational organised crime or organised crime syndicates in the convention. There are numerous components of organised crime that may or may have not appeared in every case and may altered over time, making a definite consensus definition problematic. An "organised criminal group" has been defined by the Convention (Article 2a) using four criteria:

- 1) A three-person or greater organised group;
- 2) For a limited time, the group exists;
- 3) It collaborates in order to conduct at least one or more significant crime and
- 4) To get a pecuniary or other tangible profit, either directly or indirectly.

The scope of organized crime today, along with the individuals, organizations, and networks involved, seems to be almost limitless. Organised criminal activities include crimes such as fraud, money laundering, theft, counterfeiting, and piracy (Costa, 2010). Investigations in the past have shown that in addition to various organised crime syndicates leader those who organized and masterminded crime, the political elite, serving members of the army and the police service, government employees, investment bankers, insurance companies, accountants, clearing agents and transporters were also accomplices. Despite this, organised crime syndicates remained elusive as a theoretical concept and sociological phenomenon. Despite significant efforts to explain the motivations of organised crime syndicates, its structures, and societal impacts by academics from criminology, economics, sociology, political science, and anthropology, the study of organised crime is still in its infancy (von

Lampe, 2016) and has not yet produced a cohesive and cumulative body of knowledge (Schultze-Kraft, 2016). Regardless of organised crime becoming a multi-dimensional costly crime, according to von Lampe (2016), a major authority on the subject, the literature has no less than one hundred and eighty alternative definitions. According to the UNODC (2022) organised crime syndicates swindled United States of America eight hundred and seventy billion in 2009, accounting for fifteen percent (15%) of global trade, with overall illicit revenues totalling nearly USA dollars two point one trillion. Given that the world has become not less but more connected since then as a result of globalisation processes and technological advancement, it is possible that recent estimations would be significantly higher. Money and other material gain are frequently cited as the primary reason for groups of people to organise and participate in criminal operations, which are primarily concerned with providing private 'protection' in illegal or illicit marketplaces. Identified characteristics and traits of organised crime syndicates included financial gain with corruption serving as a shield for organised crime operations. To defend the illegal operations, intimidation, threats, and or force were deemed necessary. As a continuous criminal enterprise, these factors make up organised crime. The UNODC (2009) posited that, the fact that organised crime is "structured" is the most obvious contrast between it and other forms of criminal behaviour. Random, unplanned, individual criminal activities are not included in this definition. Instead, it focused solely on deliberate, reasoned actions that reflect the collective effort of individuals. Several attempts have been made to elicit similar characteristics in order to better explain and define organised crime. The structural approach to understand organised crime syndicates focused less on individual behaviour and more on the role of bigger systemic elements including the international system's sociological, legal, economic, and political features. These elements do not inherently cause crime, but they do provide the environment for organised crime to thrive.

The fundamental "illegal-enterprise paradigm" (Kleemans, 2012) organized crime has recently come under criticism, even though the United Nations Convention on Organised Crime established a minimal level of international agreement on what is organised crime, it is not supported by enough data that concluded that members of criminal organisations engaged in "rational, profit-driven entrepreneurial" operations, while illegal, are governed by the same supply and demand laws as legal businesses. According to Kleemans (2012), the rational that organised crime is directed and coordinated by an invisible hand is unfounded, actors and leaders within organised crime syndicates are the usually untouchables, though operating in

secrecy. In essence, organised crime is about criminal cooperation in the face of adversity. The invisible hand of social relations, as well as the invisible hand of manipulation and violence, is considerably more essential in such circumstances. The hierarchical model of organised crime characterised organised crime as coordinated, interdependent and interconnected players with a defined hierarchy that differentiated the front leaders from other members of the criminal organisation. The "bureaucratic", "corporate", or "organisational" model of organised crime has been coined to describe this structure. This depiction of organised criminal syndicates mirrored that of state security organisations such as army or government-like entities structures in which unlawful acts are planned and approved by the appointed commanders then cascaded down for implementation and operationisation by lower rank or structures (Albanese, 2015; von Lampe, 2016). Official reports accepted the hierarchical approach to organised crime groupings, and it was extensively utilised to profile different types of organised crime syndicates beyond mafia style lead syndicates. This depiction shaped how organised crime was regarded and dealt with around the world (Lavorgna, 2016). Governments, non-governmental and international organisations, and academia have all conducted studies on the models of organised criminal syndicates over the years. The findings reveal that, while the hierarchical model describes some organised criminal syndicates, there are many more that are not (Lombardo, 1994; Lupo, 2015; Rostami, Mondani, Liljeros & Edling, 2017). Highly organised and hierarchical mafia groups existed on one end of a continuum of organised criminal groups, according to research, "with a variety of hybrid possibilities in between" (Sergi, 2017; Smith, 1980). The hierarchical model is particularly useful for defining how various individuals; groups organise and operate in terms of operational posts, territory, and the value of being "connected" to the group. The belief that identifying and ring fencing of organised crime leaders possibly through arrest and conviction will contain and or abolish organised criminal groups entirely by collapsing organised crime syndicates was an unintended result of widespread adherence to the hierarchical model of organised crime. Many successful organised crime syndicates criminal cases seized with the judiciary to date havenot discovered that the on-going demand for unlawful goods and services has led to the creation of new leaders and illicit organisations to exploit these lucrative illegal markets.

Frank, Perri, Richard and Brody (2011) contend that, irrespective of organised crime syndicates having their own hierarchy, studies point out that, in some cases, organised crime

syndicates operate in conjunction with terrorist groups. Criminal organisations exist to maximise earnings from illegal operations that undermine and exploit the general public's unlawful economic activities and pursuits. Terrorist groups, on the other hand, may require funds to carry out their operations, but their goals are to kill and maim targets for political and or religious reasons. On that note, terrorist and organised criminal groups are likely to interact through shared tactics and methods, the process of evolving from one kind of group to the other over time, and transaction-based service for hire operations (Mullins, 2009). Where a government's law enforcement agents and legislation are weakest, where "shadow" economies abound, and where corruption and regional strife are common, crime-terror links are more likely to occur. This syndrome can lead to a state being ruled by a criminal-terrorist organisation that makes large sums of money through fraud and corruption while preserving power through terrorism. Mortgage fraud, philanthropic fraud, identity fraud, insurance fraud, and immigration fraud are all examples of the fraud-terror nexus. These relations have allowed and enhanced the sharing of technology that can be used to advance criminal activities. Criminals quickly adapt to new technology and incorporate them into their methods of operation, or they establish totally new business models around them. Organised crime group's usage of new technology has an impact on criminal operations across the range of serious and organized crime. This encompasses online advances such as the increase of online trading and the general availability of encrypted communication channels, as well as other aspects of technological innovation such as more affordable drone technology and sophisticated printing technologies. Technology has become an integral part of most, if not all, of the criminal activities carried out by organized crime groups, giving them unprecedented flexibility. The usage of advanced information systems is no longer limited to hackers and coders; it now includes drug dealers, extortionists, and illegal gamblers as well. The Internet gives users a sense of anonymity. In turn, anonymity breeds depravity. Organised crime is always drawn to vice, and it is only too eager to take advantage of it. All of these major criminal operations have one thing in common: when technology is used to facilitate them, they become easier to carry out and more efficient. A rapidly developing criminal threat exists in the space between traditional criminal investigations and core intrusion-focused cyber investigations, where criminals are employing high-tech tools built by others and exploiting particularly complex capabilities available via the internet. The future of organised crime investigations will be determined by these techniques and technologies.

According to Albanese (2015), crime behaviours exhibited by organised crime groups have been categorized into four categories. These are organized crime, corporate crime, political crime, and white-collar crime. Organizational and white-collar crimes, on the other hand, have more similarities than distinctions, according to the study. The sole distinction was that white collar crime is an illegal divergence from legal business standards, but organized crime is a "continuous criminal enterprise" that exists to profit from illicit activities (Albanese, 2015). Groupings formed for the purpose of instigating varied forms of crime were better classified as organized crime rather than white-collar crime. The NICB published a report in 2012 that looked into claims filed by the insurer representatives and the entire insurance industry with regards insurance fraud crime perpetrated by organised crime syndicates. The most common reason for being referred to the NICB was a staged or caused accident, which accounted for over thirty-three per cent of all organised crime syndicates activity claims (McClain, 2012). A fabricated, staged vehicle collision is one that is produced or caused by the people involved in order to cheat insurance companies of claimed vehicle damage and stated medical care. All damage and injury in a staged accident are produced and reported exclusively for the goal of benefitting from a bogus insurance claim. Complex companies are often formed on the staging of such incidents. Because they create a hierarchy of individuals with well-defined positions, these firms resemble organised criminal activity.

Most staged accident businesses, according to the NICB, have at least four fundamental tiers in their hierarchy. The crash participants are the first level of individuals (NICB, 2012). These people are given a little fee to take part in the accident and file the subsequent claim. The recruiter is the next rung in the hierarchy (NICB, 2012). A recruiter is in charge of gathering the participants and, in most cases, orchestrating the accident. He's also in charge of directing the participants to the medical clinic where they'll be treated. The professional, usually attorneys or medical providers, is the next rung in the hierarchy (NICB, 2012). Depending on the company, an attorney may have a variety of positions within this structure. While some lawyers only offer legal services in exchange for bribes, others have more significant roles within the business. For instance, certain lawyers might suggest that people visit particular clinics connected to the ring. In these enterprises, medical professionals lend their license as a fictitious clinic owner or treat participants in staged accidents, send bills for non-rendered medical services, sign blank treatment forms, or treat participants in staged accidents. Next up is the ringmaster (NICB, 2012). The owner of one or more of the

associated medical clinics, as well as the billing company in some cases, serves as the ringleader frequently. The Russian mafia, the Cuban organized crime scene, and other large crime syndicates are only a few of the classic criminal groups that these leaders have ties to (Kestin, O'Matz, & Maines, 2014). In order to charge insurance companies for erroneous claims related to staged incidents, staged accident companies usually build medical facilities. These clinics frequently don't offer therapy and don't have goals in line with those of a legitimate company. According to The NICB, (2012) they merely serve as a front to the insurance industry and law enforcement in an effort to give legitimacy to claims made using a phony clinic's name and address. These staged accident firms are made up of a well-organized criminal hierarchy and companies that operate specifically to facilitate illegal activities. They collaborate with white collar experts. Despite having a crucial part in the organization, actual professionals are no different from other, more well-known organized criminal organizations. Staged accident rings should be seen to be a form of organised crime, and efforts to comprehend and deter them should follow the same rules as other forms of organised crime.

The Association of Fraud Examiners (2018) identified numerous types of insurance fraud schemes in which organised crime syndicates can take advantage of and these include:

- 1) Insurance fraud facilitated by brokers and agents;
- 2) Underwriting irregularities;
- 3) Automobile insurance fraud;
- 4) Property fraud;
- 5) Life insurance fraud;
- 6) Liability fraud;
- 7) Health insurance fraud, and
- 8) Worker's compensation fraud.

2.5 The Fraudster

A fraudster is a person who participates in unlawful tricky practices to accomplish monetary or another individual gains. They could mimic someone or stunt others into uncovering private data (Criminal Investigation Department, 2020). Fraudsters can focus on a few unique

enterprises and utilize a wide range of strategies, depending with the degree of safety in that specific industry. It is possible for insurance brokers, insurance policy applicants, existing policyholders, third-party claimants and suppliers themselves to act unlawfully. Individuals who perpetrate insurance fraud include:

- Organised criminals who commit massive financial crimes by using dishonest commercial methods;
- Professionals and technicians who overcharge for services or provide services that are not rendered and
- People in the general public who want to pay their deductible claim or who perceive submitting a claim as a chance to make some extra money.

All industries are impacted by insurance fraud, but some are more exposed than others. Healthcare, employee compensation, and auto insurance are amongst the most prone to insurance fraud (Insurance Information Institute, 2022). In order to protect insurers and consumers, the insurance business in the United States has cooperated with numerous industry organisations, intelligence agencies, and state governments to help develop systems to detect and counter fake claims. The creation of a national fraud academy is one result of this collaboration. The NICB, the Federal Bureau of Investigation (FBI), the American Property Casualty Insurance Association (APCIA), and the International Association of Special Investigation Units worked on the establishment of the academy. Its purpose was to educate and train fraud detectives in the fight against insurance fraud. The capacity to profile, characterize and undercut the fraudster, according to the school, is the most significant capability in preventing fraud. Understanding the reasons why individual or groups commit fraud has helped to guide and design effective insurance fraud prevention and countermeasure measures. It's vital to note that, in addition to profiling, comprehending insurance fraud motivation can be difficult, especially when just fraud offenses are deemed a national security danger (White, 2010). A discussion by Cressey's (1953) 'fraud triangle' was and is frequently included in a dissection of fraud motives, the motive of individuals or a group to conduct financial crimes, including insurance fraud. The fraud triangle included or specified the factors required for fraud to occur, which in the case included a motivated perpetrator, a fraud opportunity, and a rationalization that soothes the crime. With the advancement of technology, however, a number of new factors have evolved.

Anyone has the potential to perpetrate insurance fraud, particularly in financial transactions. Investigators and intelligence agents have created profiles of how fraudsters behaved. Despite the fact that there has been several research on insurance scammers, they have however, generally escaped scholarly notice. There is little information available regarding how they view the risks involved or why they have favoured insurance fraud over other types of illegal crimes. Fraud is a crime that involves deceit and concealment; in practice, it encompassed a vast range of acts that are independent and perpetrated by a diverse set of individuals (Dobie, 2012). Offenses involved a wide range of acts, such as employees cheating their employers (Gill, 2005a; 2007). Other examples included large-scale theft or low-level criminals 'fiddling' cross-border fraud (Button, 2012); identity theft and fraud; advanced fee fraud (Smith et al., 1999); and insurance fraud (Smith et al., 2010). Similarly, there have been numerous types of insurance fraud cases that have been investigated by intelligence officers and other related government entities (Palasinski, 2009). Insurance fraud, according to the Association of British Insurers (2012), covers offenses committed by individuals against persons, individuals against organizations, and organizations against individuals and other organizations. It is crucial to note that the linkages between fraud and organised criminal syndicates are well-known (Levi, 2012). Insurance fraud is divided into three categories, according to the Association of British Insurers (2012). The first is opportunistic insurance fraud, which comprises inflated and faked claims in general and retail insurance. The second type is opportunistic fraud in commercial insurance, which focuses on companies rather than individuals that perpetrate fraud. Organised fraud, on the other hand, involves organised crime syndicates. There is a significant distinction between opportunistic fraud, which occurs when people see a chance to perpetrate fraud in their regular lives, and more organised planned fraud. Insurers may also be victims of their own employees taking advantage of opportunities or meticulously preparing ahead of time, sometimes partnering with outsiders who may be former employees, albeit this is only seldom characterised as insurance fraud. New fraud strategies are always being created, and businesses must adapt by updating their defence mechanisms.

The insurance industry has long been known for having the highest rate of fraud (Levi, 2008), and there are at least four reasons for this. Insurance fraud has an enigmatic nature, and its techniques are always becoming more complicated and sophisticated. Insurance fraud has grown more to be difficult to identify and quantify in terms of financial damage. Insurance

fraud can happen at any time during the course of a transaction. According to the Association of Certified Fraud Examiners' (2012), insurance fraudsters profiling training manual, fraud offenders were most likely to be discovered in one of six divisions in an insurance firm. These were accounting, twenty-two per cent, and operations seventeen per cent, sales, thirteen per cent, executive or upper management, twelve per cent, customer service, seven per cent and purchasing, six per cent. A study by an insurance company, according to the Association of Certified Fraud Examiners (2012), confirmed that individuals between the ages of thirty-one and forty-five years are usually involved in cases of insurance fraud either working as an individual or as an organised crime syndicate. Button et al. (2013) asserted that household insurance fraudsters are almost likely to be male in some cases, female aged between thirty and fifty years with a mean age of forty-four years, and from a variety of occupations. The Zimbabwe Republic Police (2022) also noted that the age group might reduce to twenty years particularly in male criminal syndicates. Furthermore, 2019 intelligence briefs to the Commissioner general of the Zimbabwe Republic Police, pointed out that fraudsters involved in various fraud related crimes including insurance fraud have attempted by all means to maintain a clean criminal record and, in some cases, they bribed state security agents to have their criminal record cleared at the Zimbabwe Republic Police Central Criminal Records Bureau (ZRP-CCRB). However, intelligence gathered by the President's Department (2020) revealed that there are notable links amongst individuals or organised criminal groups involved in insurance fraud, with most of them exhibiting red flags behaviours such as unusually close association with insurance agents, vendors, politicians and policyholders. Intelligence further explained that, irrespective of these criminal offenders having their criminal record cleared, they are usually involved in a series of related crimes and schemes which include skimming, cash on hand fraud, payroll fraud, cash larceny, check tampering and register disbursements. Other cases include corruption, billing schemes, expense reimbursement fraud, fraudulent statements and other non-cash fraud.

The Zimbabwean intelligence community acknowledged the fraud triangle as a point of departure in trying to understand the motives and or causes of insurance fraud. According to Levi (2008), some sorts of fraud, such as adding items to those properly taken in a burglary, need specialist skills and access to networks of adequately skilled co-offenders, whilst others, involving modest levels of competence, can be perpetrated by regular people. This theory holds true for insurance fraud as well. In the majority of insurance fraud cases discovered,

fraudsters or organised crime syndicates leverage on their knowledge of the insurer's inadequate internal processes, such as lack of artificial intelligence, failure to verifying claims and concentrating on areas auditors usually do not prioritise. With this information, potential fraudsters and already existing fraudsters can do replica payments. Eight (8) factors that contributed to insurance fraud were identified and collaborated from the document inspections on insurance fraud criminal cases, this was following investigations and intelligence gathered by the intelligence community, namely the Zimbabwe Republic Police Criminal investigation Department (CID), the Intelligence Community which comprises the President's Department, Police Internal Security Intelligence (PISI) and the Zimbabwe National Army Military intelligence Department (MID) and various insurance companies for the period between the year 2015 to 2020. The factors include inequitable remuneration, perceived reward, and the existence of an opportunity, conspiracy, and access to the systems of the targeted insurance company, presence of an initiator, safety and justification. The presence of these factors enhanced the chances of individuals or organised crime syndicates to consider and continue with insurance fraud. It is important to also note that the exclusion of one of the factors acted as a hindrance factor as well.

The question of whether it is possible to develop a fraudster profile that is accurate enough to detect thwart a threat of insurance fraud and also to design countermeasures has been debated for a long time by the fraud experts, state intelligence apparatus and the academia. Artificial intelligence, at least for the first time has profiled the prediction mechanism to detect and red flag possible fraud schemes before the crime is committed. However, understanding the ever-changing nature of fraud and the fraudster through profiling helped the insurance industry to strengthen their defences against the illegal activity. An analysis by KPMG of five hundred and ninety-six fraudsters and organised groups investigated between 2011 and 2013 revealed that the interaction between the fraudster and the operating environment is evolving. Both fraud types and fraud scammers are constantly changing. One significant issue that worried insurance companies and other organisations is the rising use of technology by fraudsters. This is not exclusive to nations with developed technology infrastructure like the USA and the United Kingdom. It is a worry for all businesses since there is a new generation of people who are able to use advanced technology and have access to considerably more information than previous generations. All of this, however, has heralded a new era of deception and unlawful activity.

In that regard and in addition, to design effective counter measures, the intelligence community has highlighted that is of great importance, crucial to know if personal or environmental factors are more powerful predictors of fraudulent behaviour. Fraud investigations (and fraud risk management) has focused on the fraudster's personality, determining if personal elements are dominating. To note, if environmental circumstances played a major role in the fraud, the inquiry would have focused more on those areas to figure out how it influences fraud. An understanding that environmental and personal factors acted as a combo was reached. Additional classified intelligence identified and grouped four (4) drivers namely opportunity, motivation, rationale and capability, with capability as a subset of opportunity taken into account. The first two categories are environmental factors, and the latter two are personal attributes. Internal controls that contributed to the fraud's persistence are frequently exploited by fraudsters. Internal control, on the other hand, is not a significant factor in determining whether or not someone will engage in corrupt or criminal behaviour, such as fraud. According to the Criminal Procedure and Evidence Act (2019), corrupt behaviour involves at least two people, a concept known as conspiracy, and at least one of them is rarely subject to internal controls. With the increased globalisation of businesses, it is becoming increasingly difficult for any central office to keep track of what far-flung departments are doing and what threats they are facing. The aspect of employee motivation was also not underestimated; employee remuneration plays a crucial impact in moulding employee behaviour, according to a 2020 report by the Insurance and Pension Commission. Start with a pay equity audit for company leaders and boards to guarantee that their organisation is paying employees fairly; failure will result in employees compensating themselves through occupational fraud.

Evidence forwarded by the President's Department (2021), criminals does not just commit fraud, but they follow a fraudster's decision-making circle. The decision-making cycle is made up of five continuous stages. Figure 2. 2 below exhibits the fraudster cycle.

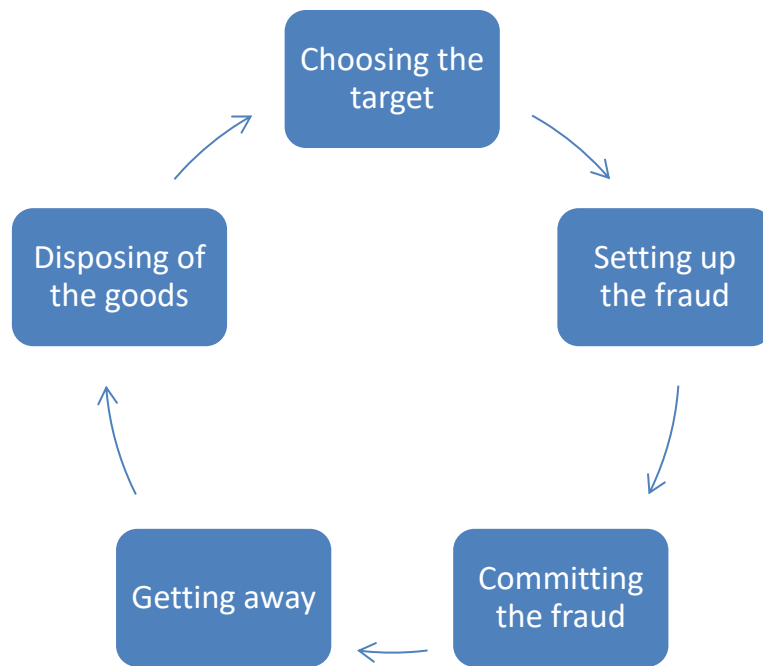


Figure 2.2: The fraudster cycle

Source: Owner's Compilation

According to the fraudster cycle, choosing the target is the departing point for any form of crime, but this is particularly important in organised crime. There are several factors considered by the fraudster before targeting the insurance company. In that regard, the fraudster goes on an intelligence gathering mission of the insurance company. Vulnerability is the most crucial aspect organised crime syndicates take into account when targeting, issues to do with internal counter measures such as artificial intelligence, policies and procures including employee awareness and alertness are all considered. Setting up the deception comes second. Criminals are opportunistic; hence they require some planning or strategy. A legitimate claim may present an opportunity for certain people who have never before committed fraud. Some criminals are continually looking for new ways to defraud others. Finch (2011) noted that prospect of being discovered is generally viewed as a more substantial deterrent. Conducting the crime is the action phase of the cycle. The risks are enhanced when obstacles are placed in the way of fraudsters readily conducting crimes, and notably when they are delayed in climbing or evading those obstacles and or leave evidence behind. This way of thinking could inspire a variety of insurance fraud prevention strategies. Finally, the products must be disposed of. This may or may not be significant depending on the type of fraud. After all of this is considered, a variety of factors are taken into

consideration to determine whether or not an offender will succeed. One of these is the quantity of resources they have at their disposal to commit the crime and get away unnoticed. Research on the resources needed for criminal action vary and applied to various crimes including insurance fraud (Gill, 2005).

2.6 Cost and Threats of Insurance Fraud

2.6.1 Cost of insurance fraud

Insurance fraud accounts for a large portion of the revenue created by the insurance industry. Money exchanged by insurers locally, regionally, and globally to settle claims has a large percentage owed to insurance fraud. According to the Association of British Insurers (2019), in the United Kingdom alone, insurers discovered one hundred and seven thousand fraudulent insurance claims costing one point two billion British pounds in 2019. A new scam is discovered every five minutes, with insurance fraud cases totalling three point three British pounds on a daily basis. The cost of insurance fraud has been and is extremely a challenge to estimate with precision considering that other insurance fraud cases go undetected and others go unreported. Conservative estimates by the Coalition against Insurance Fraud (2020), yearly insurance fraud losses are estimated to reach eighty billion USA dollars although the true figure could be substantially higher due to COVID-19 health insurance fraud. Currently, corona virus-related fraud is increasingly spreading across the globe, the USA alone has recorded more than two hundred and twenty-nine thousand, six hundred corona virus (COVID-19) fraud complaints scams, targeted victims have reported losing USA dollars thirty-eight point six million with a median loss of USA dollars four hundred and seventy (Federal Trade Commission, 2020).

New technology emerging, which is also available on the commercial market, has become handy for organised crime syndicates who are targeting micro insurance service providers. Organised crime syndicates have had access and use of full suite of scam technology; thus, they have become quite sophisticated and creative hence this has given organised crime syndicates capabilities to also conceal their identity (Reinsurance Group of America, 2019). Customers have been victims of fraud, whether low-tech or high-tech, hard or soft, or organised. While fraud has constantly evolved and affected all types of insurance, the National Association of Insurance Commissioners (2020) investigations revealed that between 2019 and 2020, organised criminal syndicates actively manipulated the COVID-19

pandemic to their advantage, making health care insurance fraud the most common in terms of frequency, followed by automobile insurance fraud and employee compensation fraud perpetrated by both employees and employers. According to the Association of Savings and Investments South Africa (2018), insurance fraud has been one of the major challenges that the insurance industry perpetually faced as up to thirty-two per cent of all claims submitted in any year in South Africa could be fraudulent, and almost a third of claims are perpetrated by organised crime syndicates. South African Standard Bank (2018) valued the rate of short-term insurance fraud in South Africa at a cost of which is around fifteen per cent of premium costs and these costs are directed to the public by way of increased premiums. With organised crime syndicates going hi-tech, insurance fraud claims are expected to rise in South Africa from three billion rands to more than ten million rands annually (Johannesburg summit on fraud, 2017). The South African Fraud Prevention Services (2017) revealed that between 2017 and 2019 new fraud cases registered on its databases increased by thirty per cent annually. In comparison, the USA, insurance industry, made up of seven thousand service providers collects an estimate of USA dollars trillion in premiums annually (FBI, 2018). The massive size of the industry has been vulnerable to criminal syndicates not only because of poor countermeasures but by its sheer size which provided more opportunities and bigger incentives for committing illegal activities. Insurance fraud costs more than USA dollars forty billion per year, excluding non-health insurance, and policyholders lose between USA dollars four hundred and seven hundred dollars per year in the form of increased premiums on average. Taking Zimbabwe as an example, the insurance business loses close to USA dollars one hundred and sixty-five million dollars per year due to fraudulent activities carried out by organised criminal syndicates (Karonga, 2017). The Zimbabwean government is currently working on modalities to establish an insurance fraud unit that will house intelligence officers and law enforcement agents. The unit will be responsible for detecting and investigating cases of insurance fraud which is on the rise in the country. Old Mutual Zimbabwe senior business development manager, Musonza (2018), highlighted that thirty to forty per cent of claims put forward by insurance policyholders were fraudulent, threatening the viability of insurance companies in Zimbabwe. Over the year, Insurance and Pension Commission Commissioner Karonga (2013) revealed that organised crime syndicates targeting insurance companies offering services to low-income markets have and are perfecting their tactics. Air Zimbabwe lost over USA dollars ten million between the years 2009 and 2013. Syndicates' insurance fraud also accounts for the loss of USA dollars nine

hundred thousand from a local authority's pension fund. Further, an average of USA dollars one point five million is lost annually by each insurance company due to exaggerated claims; particularly health claims (First Mutual Holdings, 2015).

Coalition against Insurance Fraud (2018) braked down insurance fraud statistics by industry, giving a quick overview of the costs associated with insurance fraud. Every year in the USA, false claims amount to at least eighty million dollars. Property-casualty fraud steals more than thirty million dollars each year. Insurers pay out more to ten percent of their claims costs in fraudulent insurance fraud claims every year. At least one in ten small business owners are concerned that their staff will invent workplace injuries. The essence of insurance fraud is cryptic, and its operations are becoming increasingly complex and sophisticated every day. In terms of financial impact, insurance fraud is difficult to detect and measure. The values given above fluctuate from year to year for a variety of reasons.

Statistics on insurance claim fraud revealed that determining the true cost of insurance fraud is a challenge. Fraud prevention is a component of scams that extends beyond the payment of fraudulent claims and expenses. When we looked at from an eagle eye's view, it'sclear that fraud not only cost policy holders' money and caused unnecessary inconvenience, but it also stifled innovation. During an insurance transaction, fraud can occur at any time. Insurance applicants, policyholders, third-party claimants, professionals that offer services and equipment to claimants and insurance agents can all be portrayed as protagonists in typical fraud schemes. One or more of the following factors are present in the majority of insurance fraud cases:

- Inflating a real claim or padding insurance claims;
- Making false statements on an insurance application;
- Filing claims for damage or injuries that never occurred, services that were never rendered, or equipment that was never supplied and
- Accident staging.

2.6.2 Health Insurance Statistics

Each year, around four billion health insurance claims are processed in the USA (National Anti-Fraud Association in Health Care). The fact that some of these health insurance claims are bogus is undeniable. Despite the fact that they account for a small percentage of all

insurance claims, each false claim is costly. Surprisingly, immediately after the 2010 healthcare reform bill which made inexpensive health insurance available to more people, the Secretary of Health and Human Services warned the public about a proliferation of fraudulent health insurance coverage.

In order to file false insurance claims for reimbursement, the most common health insurance frauds target patients by adding fictitious diagnoses to medical records. According to estimates, three to ten per cent of all healthcare costs are fraudulent. Both the public and private sectors are susceptible to fraud. The USA healthcare system lost between eighty-one billion and two hundred and seventy billion dollars to fraud in 2011, as according to figures from Public and Commercial Health Insurance. The National Health Care Anti-Fraud Association (2011), USA dollars two point two septentillion dollars was spent on healthcare, with three to ten per cent of that amount coming from false claims. Deception occurred at numerous locations in the system. In incidents of health insurance fraud, not only hospitals, nursing homes, and diagnostic centres were named as victims and accomplices, but also doctors, nurses, medical equipment suppliers, and even attorneys. In 2018, five point one billion healthcare robocalls were made (Coalition against Insurance Fraud, 2018). According to a 2018 survey by the USA Sentencing Commission, most Americans connected spam calls with displeasure. There was more to these annoying calls, though. Consumers were the primary target, with the goal of selling them bogus health insurance or needless medical equipment. By providing any personal information via these robocalls, the individual was putting oneself at risk of medical identity theft and other health insurance fraud related risks. Many instances of medical insurance fraud involved a robocall, according to statistics on the subject. In most situations, these malevolent arrangements created a platform for health insurance fraud by using personal medical information obtained through scam calls. The robocall was used in several cases of health insurance fraud. In the fiscal year of 2018, the Zimbabwe Republic Police convicted four hundred and twenty-five healthcare offenders who used a robocall; the number increased during the corona various to seven hundred and twenty monthly.

2.6.3 Automotive Insurance Fraud

Premium leakage only in the USA was twenty-nine billion dollars in the vehicle insurance industry (Verisk Analytics, 2019). Premium leakages were defined as insufficient insurance and lower premiums due to the omission or misrepresentation of underwriting information.

Premium leakage can occur at any point during the policy life cycle, according to automobile insurance fraud statistics. Two of the most common plots involved applicants intentionally distorting information and agents pressuring claimants to alter the facts in order to lower their rates. According to the Insurance and Pension Commission (2019), one out of every ten Zimbabwean supplied false information or omits essential data when purchasing auto insurance. According to statistics on fraud, destruction, and deception, forty per cent of Zimbabweans reported less annual driving kilometers, and twenty-seven per cent chose to leave a driver off the record. Other interesting car insurance fraud statistics show that ten per cent of people entered the incorrect ZIP code when explaining where the vehicle would be stored. One out of every ten respondents also reported that their family car or motorcycle was kept in a garage when it wasn't. Fraud-related overpayments in auto injury claims totalled between USA dollars five point six to seven point seven billion. The majority of these fraudulent claims, according to insurance fraud statistics, were chiropractic treatments, physical therapy, and alternative medical services. To put it another way, auto accident claim fraud and abuse accounted for thirteen to seventeen per cent of all pay outs for auto injury coverage. On the other hand, the true cost of car insurance fraud is far higher, resulting in higher premiums and fewer benefits for everyone. Personal injury protection insurance (PIP), sometimes known as no-fault insurance, compensated for medical expenses and permitted policyholders to sue their own insurance company for financial losses. It made no distinction as to who was to blame for the accident.

2.6.4 Scams in Life Insurance

During the contestability period, about twenty per cent of life insurance claims were denied. The contestability period is the time during which an insurance company analyses claims and has the option to deny if life insurance fraud or misrepresentation is discovered. The time might run anywhere from one to two years and begins as soon as the policy is implemented. When only insurance issued to younger insured are considered, the percentage of denied claims raised to about twenty per cent. The insurance sector loses between USA ten and twenty billion dollars each year due to life insurance fraud (Reinsurance Group of America, 2019). Medical deception, agent fraud, and criminal fraud were the most alarming types of fraud, according to respondents in a Reinsurance Group of America. Paramedic fraud and rebating ranked first and second in terms of the most difficult scams to uncover.

2.6.5 Statistics on Property and Disaster Insurance Fraud

Insurance fraud robbed the USA dollars of sixty to eighty billion. Massive wind damage and severe flooding, as well as the historic Hurricane Katrina, paved the way for widespread insurance fraud. Approximately one hundred billion dollars in damage was caused by the storm, and approximately one point six million insurance claims were lodged, totalling thirty-four point four billion dollars in insured losses. The natural disaster clearly created numerous opportunities for insurance fraud. Apart from staged natural phenomenon insurance fraud, persons who purposefully started fires become a source of insurance fraud scams (National Fire Prevention Association, 2019). Property or renters' insurance offenders set fires on purpose for a variety of reasons. Crime concealment, excitement, radicalism, vandalism, retribution and, of course, profits were only a few of them. Insurance arson is an example of a crime motivated by the prospect of monetary benefit. Statistics reveal that most insurance fraud fires are started to destroy properties, dissolve enterprises, and damage inventories in order to collect insurance benefits. Property damaged from arsons has resulted in huge amounts claims. Arson data are difficult to track, according to the Coalition against Insurance Fraud. However, there is enough evidence to conclude that arson assaults against residential and commercial properties to secure insurance benefits have decreased in recent years. Property damage from arsons totalled to USA dollars one point three billion yearly.

2.7 Threat of Insurance Fraud

The Criminal Law and Codification Act of Zimbabwe (2000) categorised insurance fraud as a serious and prosecutable offence. According to Chapter 9 subsection 24 of the Money Laundering and Proceeds of Crime Conduct (2019), a predicate offence is a criminal act that can be used to support numerous criminal acts such as money laundering and terrorism financing (Zimbabwe Law Society, 2017). Organised crime syndicates operate globally, conducting various criminal activities including fraud, drugs, arms and human trafficking, cybercrime and terrorism. Billions of dollars of money obtained via insurance fraud are wired across the world annually, distorting economies, corrupting government officials, law enforcement agents and vital government institutions and as well as fuelling civil conflict. Globally, organised crime has become a major issue on security intelligence briefs and security affairs, a crucial factor with a direct impact on international economy, security and an immediate reality for governments, legislators, intelligence personnel, law enforcement agents and general public globally. Aside from the direct effects of financing terrorism and

insurgency, drug, human and arms trafficking, cybercrimes, environmental damage and various organised crime activities that can undermine the rule of law and good governance, without which there can be no sustainable development (United Nations, 2019). The Director-General of the President's department, Moyo (2020), reported that organised crime of such magnitude is increasingly becoming concealed due to the use of technology and increasingly becoming dynamic and complex that require robust, security intelligence led response to counter. Organised crime syndicates are self-perpetuating groupings of persons who operate, fully or in part, via illegal means and regardless of geography, with the ultimate goal of illegally obtaining power, influence, and monetary (FBI, 2018). Organised criminal syndicates have operated under no single structure; their organograms are not fully defined, but they range from hierarchies to clans, networks, and cells. These organisations maintain a high level of secrecy, concealing their activities through illegal means such as bribing government officials, politicians, and law enforcement agents, intimidation and violence, complex radio communication systems, and national connections and presence. With few exceptions, the ultimate goal of organised crime syndicates is to make money, and they do so through a variety of legal and illegal techniques. Drug, weapons, and people trafficking, as well as money laundering, gambling, extortion, counterfeit products, illicit wildlife trade, cultural artefact smuggling, and cybercrime, are all activities they engage in. Fraud, including insurance fraud, was and is a keystone within organised crime syndicates enterprises (UN, 2019). The large sums of money acquired through insurance fraud are then applied to the expansion of criminal operations that pose a danger to global economies and human security. With the increased availability of intelligence and security-related technology in civilian markets around the world, organised crime syndicates are increasingly incorporating cyber techniques into their illicit activities, either by committing cybercrime or by using cyber tools to facilitate other unlawful acts (CIA, 2018). This technology has also over the years enabled organised crime syndicates to engage in insurance fraud, but with a global reach (CIO, 2018). Insurance fraud is a global crime that has threatened both human security and economic development. Reportedly, a classified report within the Zimbabwean intelligence community (2018) on insurance fraud highlighted that insurance fraud affects several victims which vary from policyholders and their families, investors, and the insurance company and its employees as well as the economy at large. Insurance fraud therefore continues to be a leading national threat considering that it is, globally, an easy source to finance organised crime syndicates operations, amongst them subversion, human and weapons trafficking,

financing insurgency groups and terrorism. On-going investigations by the security intelligence apparatus in Zimbabwe have since revealed that organised crime syndicates are securing more funds illegally in the insurance industry taking advantage of the corona virus, COVID-19 pandemic (Institute for Security Studies, 2018). These funds are financing, maritime piracy operations, smuggling and transportation of cocaine, methamphetamine in West Africa alone; firearms in Mozambique; and a global illegal flow of essential medicines. Furthermore, organised crime syndicates are also financing and involved in poaching, profiteering, racketeering, tax evasion, and illegal digging of valuable minerals. However, the activities are expanding across Africa hence posing a regional threat. The investigations further categorically noted that organised crime syndicates operating in Zimbabwe are primarily targeting insurance companies offering services to low-income earners taking advantage of low if no investments in effective counter insurance fraud measures.

In that regard, organised crimes become a lucrative industry in Africa, generating USA eight hundred and seventy billion dollars, or one point five per cent (1.5%) of world's gross domestic product (GDP) (UNODC, 2010). This posed a threat destabilise Africa and the threat exist to date. In Mozambique, Somalia, and Angola, organised crime continues to undermine peace and human security; human rights are being violated, damaging societies' economic, social, cultural, political, and civil growth (International Criminal Police Organisation, 2018). A study by the Stockholm International Peace Research Institute (2019) reported that "fifteen countries were in active armed conflicts in sub-Saharan Africa in 2019, namely Burkina Faso, Burundi, Cameroon, the Central African Republic (CAR), Chad, the Democratic Republic of the Congo (DRC), Ethiopia, Kenya, Mali, Mozambique, Niger, Nigeria, Somalia, South Sudan and Sudan. Eight were low-intensity, subnational armed conflicts, and seven were high-intensity armed conflicts (Nigeria, Somalia, the DRC, Burkina Faso, Mali, South Sudan and Cameroon). Almost all the armed conflicts were internationalized, including as a result of state actors (whether directly or through proxies) and the transnational activities of violent Islamist groups and other criminal networks that provided finance, arms, logistics and other military-related technology and supplies. Apart from armed conflicts, the International Labour Organisation (2010) highlighted health issues emanating from drug abuse, politically motivated violence, insurgency and terrorism, human trafficking and migrant smugglers are all being peddled by organised crime syndicates. Millions of individuals are wounded every year as a result of organised crime groups'

operations, with two point four million of them being victims of human trafficking. Money generated through insurance fraud has been injected in various international crimes, according to a 2018 classified study published by the Inter-State, Defence, and Security Committee of the Southern African Development Community Organ on Politics, Defence, and Security Cooperation.

2.8 Consequences of Insurance Fraud

The policyholder and the insurance company are both affected by insurance fraud in one way or the other. Micro insurance fraud has immensely contributed to the increased insurance premiums for policyholders, particularly low income earners who are already financially unable to pay for high end insurance policies. When insurers pay fraudulent claims for unnecessary or improper repairs; property that was not damaged or stolen; or injuries that were not as severe as reported or did not result from a workplace accident, insurers pass the cost of such insurance fraud on to policyholders by charging higher premiums in order to meet legal capital and surplus requirements. Fraudulent claims and the cost of investigating suspected fraud have also resulted in increased rates for honest consumers, according to Insurance Europe (2019). Investigating fraud has an influence on insurers' capacity to respond rapidly to legitimate claims. Furthermore, information from insurance fraud studies suggested that finances from insurance fraud have funded and promoted other forms of serious crimes. Denmark has withheld roughly sixty-seven million (€67m) from claims payments. Fraud costed Germany more than four billion (€4b) per year, according to the estimates. In that regard, fraud added an extra fifty-eight pounds (€58) to every policyholder's annual insurance bill in the United Kingdom. Insurance Europe (2019) noted with concern that Sweden discovered a criminal ring of organised crime syndicates responsible for at least two hundred and fourteen manufactured traffic accidents. Its actions had an impact on every major non-life insurance firm in Sweden. This gave insurers gruesome task to balance between the commitments of paying all genuine claims as promptly as possible, while working to strike a balance between investigating potential fraud and ensuring that real claimants are not affected. While insurers must examine all suspected frauds, they should do everything possible to ensure that genuine claimants receive prompt and efficient payment. In typical insurance fraud cases, an insured person or company files a fake or inflated insurance claim in order to receive reimbursement for losses they did not experience. While most people are aware of the financial implications of fraud, many are unaware that it can

also result in a violent crime involving death, physical injury, and considerable property destruction (Pharmacist Mutual, 2017). When innocent motorists are lured into accidents manufactured by criminal gangs, their lives are put in hazard; homes and businesses are frequently burned down for insurance money, endangering fire fighters, family members, and surrounding properties. Furthermore, when medical professionals execute potentially harmful and needless operations on healthy patients only to enhance their billings, health care and injury-related claims can become perilous. The elderly, indigent, and homeless are typically the victims. Murdering a spouse, relative, or business acquaintance in order to collect on the victim's life insurance policy is a common strategy. According to Shorokin (2020), any fraudulent technique meant to benefit a business or an individual is considered fraud. It can be prosecuted as both a criminal and a civil offense. Micro insurance fraud is considered as easy money by organised crime syndicates, organisations, and individuals both internal and external to the organisation, at least until the culprit is caught. The repercussions can be severe at that moment. However, organisations, insurance companies and related service providers will lose money once they are victims of fraud. It is imperative to address security procedures to reduce the possibilities of future fraud affecting business bottom line.

2.9 Insurance in Developing Economies

According to the United Nations (1994), before the creation of a domestic insurance industry, the typical market in developing nations consisted of locally licenced agents or offices of global insurance organisations. This began to change as governments recognised the importance of insurance operations in the development of their economies, and as global insurers became more responsive to local issues. Since then, governments have worked hard to build and strengthen national insurance markets that explicitly meet the needs of low-income individuals. Low-income markets in developing economies are garnering business strategists' attention in ways that would have been unthinkable even ten years ago (Lloyd's 3600 risk insight 2019). In the insurance industry, poverty reduction is being viewed as an economic opportunity rather than just corporate social responsibility. It is not a novel idea to give insurance services to low-income people. In the nineteenth and early twentieth centuries, industrial insurance was the predecessor to today's microinsurance. Despite this, insurance companies have yet to discover the majority of low-income markets in Africa's developing nations. Fewer than five per cent of low-income earners have access to insurance, and even fewer have access to the necessary commodities. These are the micro-insurance markets that

are being investigated. In developing nations, the potential market for insurance policies is projected to be between one point five and three billion policies. A wide range of insurance products, including health and life insurance, agriculture, property insurance, and disaster insurance, have been and are still in high demand. Apart from profits, commercial insurers who provided micro-insurance services gained from a wider and more diverse risk pool, improved reputation, and market knowledge and innovations applicable to other company activities.

The uncertain and quickly changing economic environment has, however, made it necessary for insurance companies to develop innovative technology that enhanced insurance issuance monitoring. This was prompted by the definite tendency that had arisen toward the creation of competitive markets that adhered to market economy principles. Secondly, supervisory authorities' plaid a critical role in ensuring that these standards are followed and markets operate smoothly. Also in addition is that politicians' attitudes toward consumer protection had shifted as a result of the democratic process. Some countries' laws and regulations were producer biased until recently as a result of national economic policies, but they are currently being changed to give greater consideration to consumer concerns. This general trend is notably noticeable in perceptions of the insurance industry's handling of policyholders, beneficiaries, and third parties. The formation of public complaints sections inside supervisory organisations and ombudsmen's offices, as well as measures aimed to speed up claim settlement, show that public concerns about insurance operations are being given more consideration. Insurance is one of the services that has benefited from global trade liberalisation. Opening up emerging countries' internal markets to international rivals has had a considerable impact on market circumstances. Supervisory bodies plaid a significant role in this regard. They ensured that market access, establishment, national treatment, non-discrimination, and transparency rules arising from the implementation of the GATS (General Agreement on Trade in Services, as contained in the Final Act of the Uruguay Round) are followed and that no competition rules are broken.

In most rising countries, there are objective reasons to alter the regulatory and supervisory systems for insurance. Several emerging countries, particularly in Latin America, have already liberalised their insurance markets by making considerable changes. Supervisory agencies should take a proactive approach in this regard, suggesting to their government new legislation that is needed to adapt markets to changing conditions, as well as analyzing and

fine-tuning their execution regularly. Liberalization and deregulation are usually linked. Deregulation is defined as a reduction in regulatory activity. Certainly, "administrative harassment" should be reduced, but rather than a reduction, the overarching goal should be to offer insurance companies more autonomy in their administration.

2.10 Micro Insurance and Human Security

Human security has been and is increasingly becoming a security necessity in response to the interconnectedness and complexity of both old and new, non-traditional security threats, namely but not limited to chronic, persistent poverty, ethnic violence, human trafficking, climate change, health pandemics, international terrorism, and unexpected economic and financial downturns (United Nations Office for the Coordination of Humanitarian Affairs, 2016). Such threats frequently transcend conventional security notions that concentrate only on foreign military aggressions by taking on localised dimensions and focussing on an individual. In that regard, a comprehensive approach, utilising a wide range of new possibilities is required for human security in order to handle these concerns holistically. Traditional security solutions are incapable of addressing human security threats on their own. Instead, they advocate for a new consensus that recognises the connections and interdependence between national security, human rights, and development. Security, rights, and growth are examples of "human components" that make up human security. It is therefore a multidisciplinary, prevention centered, cross sectorial, all encompassing, and a context specific concept. As a people centred concept, human security places the individual at the centre of state security (President's Department, 2019). As a result, it considered a variety of risks to life, livelihood, and dignity as well as the threshold beyond which human life is intolerable. A multi sectorial understanding of insecurities is also necessary for human security. Therefore, ensuring human security necessitated a broader comprehension of threats, such as disturbance in the political, social, economic, and health sectors as well as the environment. The two fundamental components for reaching the goal of human security are protection and empowerment of the populace. Governments, international organizations, non-governmental organizations, and the business sector all have worked to safeguard people from a diverse of hazards (United Nations Office for the Coordination of Humanitarian Affairs, 2003). This referred to the policies, processes, and organizations in place to protect people from major and pervasive dangers. Protection, in this view, included a "top-down" approach, in that it recognised that people are exposed to perils beyond their control, such as

natural disasters, financial crises, health problems, death, business issues and conflicts. A research by the Zimbabwe Insurance Association (2018), such threats to human security affects mostly low income earners. As a result, this category of people must be safeguarded in a systematic, comprehensive, and preventative manner. Zimbabwe Insurance Association (2018) categorically recommended that it is primarily the responsibility of states, governments to put in place protective mechanism that appeals to all income level categories. On the other hand, international and regional organisations, civil society and non-governmental actors, as well as the private sector, have played an important role in the protection people particularly low income earners from risks that may emanate from different sources. In the face of hardship, empowerment also referred to strategies that assist people build resilience. In addition to protection, empowerment necessitated a "bottom up" approach. It aimed at strengthening people and communities' abilities to make informed decisions and take action on their own. While individual empowerment allowed people to not only realise their full potential, but also to design and participate in solutions that promoted human security for themselves and others.

From a security intelligence tactical approach, human security aimed at resolving complex insecurity situations by implementing collaborative, responsive, and long-term measures that are people centered, multi sectorial, comprehensive, context specific, and prevention-oriented. Human security also employed a hybrid strategy that incorporates both of these elements into a framework of protection and empowerment. In order to design effective human security strategies, the multi-sectorality and externalities framework for human security provided the necessary tools for building policy and program coherence among the relevant sectors engaging in a program intervention. By taking into account the potential externalities of the proposed intervention, the framework performed a number of critical functions in the design and enhancement of human security programs. Table 2.1 identified micro insurance as a noble and commendable human security intervention strategy that can be deployed by governments and relevant authorities.

Table 2.1: An example of a human security externalities framework

HUMAN SECURITY COMPONENTS	Possible interventions and assistance in a human	Externalities on other aspects of insecurity
--	---	---

**security field by
international
donors**

		Positive outcomes	Negative potential outcomes
Economic Security	Micro credit programmes for economic security.	Increase food production (food security). Communities saved from economic hardship less bent on fighting (political security), etc.	Competition among receiving and non receiving communities creates conflict (community insecurity). Women targeted for their increased income/power (personal insecurity)
Food security	Relief aid meant for increasing food security for communities crop and animal insurance	Can increase economic security for communities who sell their ration (economic security). Less rationale for conflict (political security), etc.	State is no longer accountable to the population but to foreign authorities (political insecurity as a result of illegitimacy). Aid is looted (personal insecurity). Aid decreases agriculture production (economic insecurity of farmers).
Health Security	(Re)building the health care system,	Balance (re)attained in mortality/fertility	Replacement of the state's responsibility

	with provision for health insurance	for rates (community and personal security). Jobs created (economic security), etc.	in providing healthcare (lack of trust in institutions, political insecurity). Sanitation not taken into account (environmental insecurity).
Environmental Security	Installing environmental management practices.	Recovering wasted and polluted renewable resources (economic security). Increased production in agriculture (food security), etc.	Ignoring agricultural traditions (linked to community insecurity).
Personal Security	Law and order interventions, increased police programmes and training (personal security).	Freedom from fear, want and indignity (with impacts on all Human security concerns). Jobs created (economic security), etc.	Replacing the state (linked to political insecurity). Abuse of power by security forces (personal and community insecurity).
Community Security	Promoting disarmament and demobilisation.	Social harmony (leading to the security of all components). Jobs (economic security), etc.	Exacerbating or creating new tensions between communities.

Political Security	Support to transition to democratic practices.	Reduction of political exclusion (community security). Participation of economic and communities (community and personal security), etc.	Imposing particular type of governance system (linked to potential community, and political insecurities).
--------------------	--	--	--

(Adapted from Tadjbakhsh & Chenoy, 2007)

Despite the fact that conceptual ambiguity is a major source of scholarly debate in the subject of human security, proponents of the paradigm argue that its most beneficial attributes are its inclusive, broad, and holistic nature (John, 2014). Human security acts as an "organising concept," allowing wide coalitions to emerge around specific "security" issues without the conventional limits imposed by restricted, state centric definitions of security, which have inhibited multi-party collaboration in the past. A holistic approach to human security definition presented such a multiplicity of security issues, where threat sources vary greatly both within and beyond states. With this complexity in mind, the only viable option was a flexible, comprehensive definition of human security. A holistic approach not only brought together diverse specialists in order to better comprehend the connections between many dimensions of human insecurity, but it also has the potential to promote international collaboration in the security, development, and human rights sectors.

2.11 Overview of the Zimbabwean Insurance Industry

For individuals and businesses, including low-income earners in Zimbabwe, insurance is a crucial component of human security and risk management. According to the Geneva Papers on Risk and Insurance (2004), insurance companies' primary duties of collecting, accumulating, and managing contractual capital savings have turned them into large institutional investors and key actors in international financial markets. Thereby playing a pivotal role in providing social security on one hand and economic development on the other. Regardless of continued technological advancements, digitalisation of global markets, and the removal of constraints, particularly government imposed economic regulations of financial

and real market; insurance companies, particularly micro insurance service providers aimed at low-income earners, will undoubtedly continue to play an equally important role in the future. The insurance sector in Zimbabwe is made up of one thousand one hundred and eighty-three registered players, all of whom are registered, monitored and regulated by the Insurance and Pension Commission (IPC, 2019). The Insurance and Pensions Commission is a government of Zimbabwe regulatory authority organisation established under Chapter 24 subsection 21 of the 2019 Insurance and Pensions Act, with the goal of regulating the insurance and pension business and protecting the interests of policyholders and pension scheme participants. Following the establishment of the Insurance and Pensions Commission (IPEC) under Chapter 24 subsection 21 of the 2019 Insurance and Pensions Act, the total assets for the insurance industry in Zimbabwe grew by forty-three point five two per cent, from USA dollars two point nine billion in 2017 to USA dollars four pint two billion in 2018. The year 2020 was a setback for insurers in the low-income cover market in Zimbabwe, experiencing pressure on their real earnings as a result of net monetary losses incurred due to the escalating cases of insurance fraud and change of currency to the Zimbabwean Dollar (“ZWD”), from the United States Dollar (“USD”) as effected by Statutory Instrument 149 of 2019. The Zimbabwean low-income cover insurance industry was also being negatively affected by the COVID-19 global pandemic which has created new avenues for insurance fraud. Insurance companies serving the low-income earners have increasingly adjudicated the claims process through digital processes in which organised crime syndicates have since exploited new fraud opportunities compounded virtual health care thereby increasing the frequency of medical fraud (President’s Department, 2019).

Further to this, efforts to contain institutional insurance fraud, major developments in the industry indicated that the Insurance and Pensions Commission has since revamped the industry’s regulatory capital requirements from being prescriptive to risk-based (Muradzikwa, 2019). Currently, Insurance and Pensions Commission has engaged African Actuarial Consultants (AAC) as the project consultant to assist in developing a risk-based capital regulatory framework in line with international standards. The project seeks to develop a framework that ensured each insurance company holds enough capital commensurate with its size and peculiar risks. The Ministry of Justice, Legal and Parliamentary Affairs (2019) also intervened in response to challenges of out dated legislation governing the insurance industry. The ministry amended the acts within the

Zimbabwean insurance industry, paying particular to the insurance act and the pension's commission acts. The envisaged amendments were aimed at aligning regulatory frameworks with the dynamic changes in the insurance sector in terms of product developments, technological changes, enhancing corporate governance, consumer protection through improved disclosure requirements, external stakeholder engagement to counter insurance fraud. The amendments also aligned insurance legislation with the International Association of Insurance Supervisors (IAIS) standards targeted at tackling contemporary issues in the insurance business in order to create a good regulatory framework that encourages the continuation of a safe, vibrant, and stable insurance industry. The South African insurance industry survey (2021) acknowledged that the insurance industry in Zimbabwe faced several challenges, amongst them an increase in cyber security threats peddled by organised crime syndicates, and poor general economic development. The cyber security threats facilitated insurance fraud emanating from the increased use of electronic platforms amongst stakeholders, with more policyholders, employees and agents working remotely. Also, low consumer confidence owed to the loss of value suffered due to hyperinflation and weak corporate governance practices all made it easy for insurance fraud. Furthermore, the insurance and pension commission (2018) noted that the absence of a policyholder protection fund and effective insurance fraud countermeasures, compounded with current inflationary pressures in the economy, have an impact on the eroding value of premiums, particularly in micro insurance.

From a security intelligence perspective in Zimbabwe, micro insurance is a social security tool that can be applied for a specific group of consumers; in most cases the government and insurance companies deploy micro insurance as a tailored service that meets the needs of low-income earners in terms of cost, delivery mechanism, coverage, terms and conditions. The inclusion of low-income earners has been at the heart of micro insurance. The Finscope survey (2014) indicated that seventy per cent (70%) of adults living in Zimbabwe do not have any form of insurance; the thirty per cent (30%) only have a funeral cover. Over the years, micro insurance in Zimbabwe is increasingly attracting low-income earners both formally employed in private entities and government employees as well as in the informal sector. In that regard, the Insurance Institute Information (2021) reported that an increased number of insurers are venturing into the micro insurance market in developing economies across Africa due to its attractive enormous number of potential policyholders. The Zimbabwe Insurance

and Pension Commission (2019) introduced the micro insurance regulatory framework, to encourage the uptake of micro insurance products. Companies, mutual societies, burial societies and cooperatives under the micro insurance regulatory framework of 2017 were and are legally mandated to register as according to the prescription of the cooperative act or relevant regulations that grants a locus standi to these service providers. This is also a prerequisite for micro insurance licenses. The focus and primary objective of the framework was the ease, cost-effectiveness and accessibility of insurance services to low-income consumers, hopping to reduce or eradicate vulnerability, protecting income streams, guaranteeing social stability and broad-based economic development. International Labour Organisation (2006) prescribed that adequate and appropriate safety nets and protection mechanisms against risks and vulnerability are an important device to reduce poverty amongst low-income earners. In developing economies such as Zimbabwe, resources dedicated to mitigating risks are very limited. Micro-insurance is aimed at Zimbabwe's low-income earners, who have remained mainly uninsured for years, as well as the need to expand financial inclusion across all socio-economic levels in the country. Micro insurance businesses that have employed this methodology have considered allowing low-wage workers in informal, public and private sectors transfer their risks across the board (Siwela, 2021). Through micro insurance, several insurance companies and mobile phone network corporations are at the vanguard of a socio-economic revolution. Unbanked Zimbabweans who are in possession of a national identity card and registered mobile phones can now use mobile money and mobile wallets to engage in the financial system.

In recent years, micro insurance has been identified as an attractive industry by insurance companies of diverse insurance services basically attributed to increasing insurance service demand and overall potential profitability of insurance products and services. Africa alone has over seven hundred million low-income Africans and is strategically positioned to be a key market for micro insurance and related insurance services. According to the Micro Insurance Network (2018) report on Africa's micro insurance landscape, barely two percent (2%) of Africa's low-income population has access to micro insurance services. In that context, insurers are coming up with innovative distribution channels for micro insurance. These distribution channels act as a conduit between the insurance companies and the most remote policyholder. Figure 2.1 below shows that Africa's micro insurance distribution channels are highly reliant on strategic alliances, with sixty-eight (68%) of micro insurance

companies employing brokerage and agency channels to distribute their services. While twenty-two per cent (22%) partner with various institutions to either directly sell the individual micro-insurance policies or bundle them with other micro-financial products, evidence in Zimbabwe is that insurance companies have migrated from stand alone and conducting their business the physical traditional method to digital business in which artificial intelligence is fused within their processes while in partnership with other service providers. Insurance companies now enjoy the ease of conducting their business through strategic partnerships with Mobile Network Operators (MNO). Strategic partnerships with Mobile Network Operators (MNO) facilitated the distribution and access of insurance products via mobile telephones and with the capacity of reaching a diverse client based including new clients based in rural areas. Such technologies become handy and reliable for low-income earners. The numerous alliances have developed as a new strategy to force insurance institutions to digitise steps in the insurance value chain process, such as premium collecting and claim payments. Among low-income earners, funeral insurance, auto insurance, health insurance, and crop and livestock insurance appear to be the most popular micro insurance products being facilitated through strategic alliances with Mobile Network Operators (IPC, 2021).

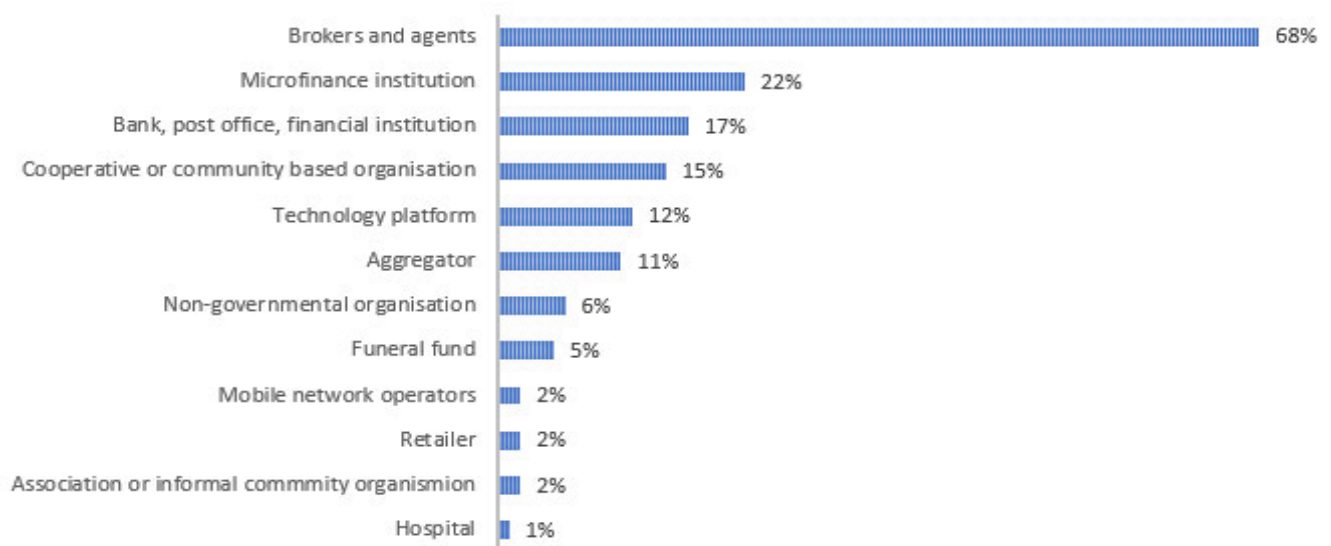


Figure 2.3: Micro insurance distribution channels

(Source: Micro Insurance report 2018 published by the micro insurance network)

The strategic partnerships and advances in artificial intelligence technology might have given insurance companies some unique capabilities, technology-based integrations in micro insurance are potential opportunities which macro insurance service providers can tap into to expand their services globally even to customer segments predominantly perceived as marginalised and in most remote areas. However, technology-based capabilities and strategic partnerships come with operational risks that were exploited by organised crime syndicates as well.

2.12 Low-income and Micro Insurance

The economic situation in Zimbabwe has traditionally allowed the rich and those highly paid mainly from the level of manager and above in the private sector and directors in a government department to have access to first class insurance services (Consumer Council of Zimbabwe, 2017). Low-income earners, in either the informal, public or private sectors, live and operate in volatile environments, vulnerable to various perils such as accidents leading to disability or deaths, theft, illness, conflagrations, natural and manmade disasters (Churchill, 2006). These low income earners are extremely vulnerable while they hardly afford to cope with the diversified risks. The numbers of low-income earners households vulnerable to risks are increasing yearly in Zimbabwe and the government of Zimbabwe have since identified the need to come up with innovative, flexible insurance products that can be stretched and accessed by low-income earners (Consumer Council of Zimbabwe, 2016). Since 1997, the Zimbabwean Government has had limited resources and capabilities to offer social protection to vulnerable citizens and has identified micro insurance as a panacea that can be applied to extend social protection to vulnerable low income earners. This has been viewed as a plausible and relevant effort in situations where a government lacks the resources and capabilities to provide social protection. In this context, micro insurance protects low-income people against specific risks in exchange for regular premium payments that are proportional to the risk's likelihood and cost (Deblon & Loewe, 2011).

The categories of low-income earners vary, but individual low income earners irrespective of industry type and employment status have since failed to afford mainstream commercial insurance by virtue of its costs and service conditions. In Zimbabwe, low income earners, also considered poor households face greater threats of insecurity. This suggests that they are more exposed to risks than their counterparts who can afford costly insurance. Low-income

earners coincidentally live and operate in informal economic sectors, unregulated, and unsafe working environments. Furthermore, the majority lack basic education, are uninformed of their social entitlements, and are underserved by prevention and health education programs; they may also live in distant areas with limited access to public social services. The insurance and pension commission in response and as a countermeasure introduced a framework that over years has encouraged the uptake of micro insurance services by low-income earners. The framework has complemented the government of Zimbabwe's policy thrusts on social protection for those in the informal sectors, particularly low income earners.

According to Article 9 of the International Covenant of Economic, Social, and Cultural Rights from 1976 and Article 22 of the Universal Declaration of Human Rights from 1948, social protection is today recognised as a fundamental human right on a global scale. The direction of developing a policy and regulatory environment that encouraged, enhanced, and facilitated the safe and sound provision of microinsurance products and services by the informal, public, and private sectors was set by the National Financial Inclusion Strategy, which identified insurance as a key player in the financial services sector and social protection. Realisation that low-income earners in Zimbabwe, including former civil servants who relied on tax-funded pensions and partially government-funded medical assistance in state hospitals, as well as employees in the informal sector, both rural and urban areas, lacked access to and did not afford formal social protection schemes, hence instead relied on assistance from friends, family, and neighbours. Non-formalised social protection programs were considered pivotal and are still vital, but they are limited in scope and quantity. The aspect of offering required service to low income earners was however, considered insufficiently dependable for those in need because the services founded on a formal obligation rather than a moral one (Deblon & Loewe, 2011). However, the most reliable option to get out of such dreadful position was through micro insurance service provision. It was intended to address the needs of low-income earners across all economic sectors, a population that was previously excluded went for years without having access to more dependable social safety programs to improve their risk management skills.

The micro insurance plan packages tailor made by insurance companies in Zimbabwe protected individuals and households who had little savings and whose monthly income was below that of an average earner. Such insurance services were specifically tailor-made to target low valued assets, health services, education, funeral cover and compensation for

illness, injury or death. These insurance services accessed by low-income earners were however, managed by following generally accepted insurance practices irrespective of them being offered by various entities (The South African Insurance Industry Survey, 2017). The Zimbabwean government identified low income earners as a unique constituency in the country. A constituency comprised of plus sixty-five per cent of the total population. In that regard, the Zimbabwean Government described low-income earners as the population proportion whose household income per consumption unit is less than sixty per cent (60%) of the equivalent median income of all households (Government of Zimbabwe Gazette, 2017). In Zimbabwe, low-income earners according to the Zimbabwe National Statistics Agency (ZIMSTAT), (2020) are defined as individuals whose total monthly income does not meet their total consumption expenditure. The total monthly income was below the poverty datum line (PDL), which represented the cost of a given standard of living that must be met if a person is not to be considered poor. The Total Consumption Poverty Line (TCPL) for Zimbabwe stood at four hundred United States dollars per family of three per month in August 2020 for both non-food and food items (ZIMSTAT, 2020). A survey by ZIMSTAT, (2021) highlighted that ninety-five per cent of the working population falls under the category of low-income earners. This was complemented by the World Bank (2020), Zimbabwe's working population is estimated to be six million nine hundred and eighty-five thousand, five hundred and thirty-six people, with ninety-five percent (95%) of the working people engaged in informal economy activities. Smallholder farmers in communal agriculture account for the biggest number, estimated to be four million, followed by six hundred and fifteen thousand in trade and commerce. Two hundred and ten thousand worked in manufacturing, seventy thousand are artisanal miners, one hundred and eighteen thousand worked in education, and ninety-two thousand worked in transportation. In addition to the ninety-five per cent (95%), the Ministry of Small and Medium Enterprise Development (2019) affirmed that there were an unexplained number of students and individuals who are formally unemployed, but contributed to the informal sector. Of this potential workforce, seven hundred and fifty thousand (750,000) are students while eight hundred thousand (800 000) are officially defined as unemployed, and are doubling as the labour force in the informal sector. This alone posed a security threat which has unsettled Zimbabwe since year 2000. The government of Zimbabwe has been confronted with an unsettled environment which comprised of high crime rate, mass demonstrations and urban violence and massive

migration of Zimbabwean to other countries such as South Africa and other European countries (International Organisation for Migration 2019)

2.13 Types of Insurance Fraud in Zimbabwe

An analysis of obtaining literature unearthed limitations of study and research into the threat and problems of micro insurance fraud irrespective of findings that micro insurance fraud poses a greater threat than regular insurance. However, micro insurance and micro insurance fraud have over years received greater attention amongst researchers, while government such as Zimbabwe had tasked its national security intelligence to investigate causes of micro insurance fraud and recommend counter measures considering the magnitude of the threat to human security (President's Department, 2020). Micro insurance has been durable tool to alleviate poverty among low-income earners basically by its function as a safety net for policyholders, according to on-going research the Insurance and Pension Commission (2020) tasked to come up with a regulatory framework to regulate micro insurance in Zimbabwe. The currently not so regulated micro insurance in Zimbabwe has over years created criminal cartels who have over years swindled the already disadvantaged group (President's Department 2020). However, the problem, threat of insurance fraud in low-income markets posed severe challenges to the long term viability and issuance of micro insurance services to low income earners in Zimbabwe. The persistent and increased level of insurance fraud had reached alarming levels that money obtained was financing insurgency groups in Southern Africa (Classified Security Intelligence Brief, 2012). The year 2013 to 2019, the Zimbabwean intelligence community, led by the Zimbabwe Republic Police (ZRP), conducted investigations and sting operations that resulted in the identification, arrest and conviction of a well-established, interconnected organised crime syndicate that included doctors, lawyers, chiropractors, car salesmen, insurance agents, and others in positions of trust who were involved in insurance fraud in some way, but mostly by making inflated or false claims and operating unregistered micro insurance companies (Ministry of Justice, 2019). Technological advancement has, to a great extent, aided these criminal syndicates which aggravated the magnitude of insurance fraud in the micro insurance market. Insurance professionals and service providers, mainly employees and insurance agents, also played a pivotal role in insurance fraud. Employees and agents engaged in insurance fraud by "padding", or exaggerating actual claims, misrepresenting information about the insurance process,

submitting claims for insured events that never occurred, and "staging" incidents, according to preliminary investigations.

In light of the foregoing, security intelligence as according to the President's Department in conjunction with the Insurance and Pension Commission (2018) identified six (6) types of insurance fraud in the micro insurance market of Zimbabwe. The types were internal and external fraud, intermediary fraud, opportunistic, syndicate and occupational fraud.

2.13.1 Internal Insurance Fraud

Internal insurance fraud was identified and explained in a way that portrayed that a firm commits fraud against itself. Insiders within the insurance companies, primarily employees and managers, were identified as major culprits who have committed this type of fraud by concealing facts during claims processes and conspiring with external stakeholders such as policyholders, agents, and employee representatives (Babalola, 2009). Internal insurance fraud was identified as a one threat with a potential to defraud insurance companies huge amounts. An investigation and analysis of previous cases of internal insurance fraud revealed that organised crime syndicates with the assistance of information technology experts within an insurance company attacked systems, channels and processes. They deployed advanced technology sometimes to wipe out information on claims that are corruptly obtained, hence they concealed the evidence and to some extent their identity (Zimbabwe Republic Police, Criminal Investigations Department, 2020). The role of employees has been pivotal in cases of internal fraud, employees have acted both independently or connived as a useful instrument in organised criminal syndicates (President's Department, 2017). However, internal insurance fraud was identified as a broad fraud typology in the micro insurance industry. As a result, it is a highly concealed type of crime and difficult to detect considering that employees involved in the crime were also identified as individuals involved in either destroying the evidence or as investigators (Insurance and Pension Commission, 2019). The Director General of the President's Department, Moyo (2019), mentioned that internal insurance fraud should not be viewed as a single threat, but rather this only triggers a series of crimes in which an employee over time would have acted as an enabler for a wide range of insurance fraud types. The Insurance and Pension Commission (2018) postulated that external pressures such as financial greed and bad working conditions associated with poor remuneration triggers the individual employee to commit internal insurance fraud against the employer or insurance company. Interestingly, recorded cases of internal insurance fraud in the

Zimbabwean micro insurance market are committed by long term servicing employees and university graduates who understand the internal systems of the insurance company, the inadequate and ineffective internal controls (Zimbabwe Republic Police Outpost, 2019). Further covert research conducted by the President's Department (2018) revealed that ninety-seven per cent (97%) of insurance companies offering micro-insurance services have never opted to invest in systems and processes to counter internal insurance fraud. Only three per cent (3%) do have systems in place which included artificial intelligence. However, the increased incidents of internal insurance fraud have exhibited that the systems are not adequate to counter internal insurance fraud. With capability inadequacy on red flag warning signs.

Internal fraud is however a form of occupational fraud. Occupational fraud, according to the Association of Certified Fraud Examiners (ACFE) (2019), was defined as fraud committed by employees of a company. The ACFE (2019) devised the occupational fraud and abuse classification system, often known as the fraud tree, after they identified three forms of widespread workplace fraud. Asset misappropriation, corruption, and financial statement fraud were the three main types of occupational fraud. Each of these groups is further divided into subcategories. A study by the ACFE (2020) on occupational fraud and abuse noted that, despite the shift to digital commerce by insurance companies, employee schemes have remained the same since 1999. This was based on an investigation of over eighteen thousand occurrences of occupational fraud.

Corruption was identified as one of the crime affecting the operations of business entities be it government departments or private entities in Zimbabwe. Workplace corruption had become a norm and institutionalised that employee and clients regarded it as normal and a possible means of survival. According to Zinyama (2010) the level and types of corruption varied across industries in Zimbabwe but corruption had remarkably increased in the micro insurance sector. Zinyama (2010) confirmed that this has been necessitated by the collapse of systems and countermeasures both internal and external to an organisation that is meant to counter workplace fraud. Various corrupt activities have been unearthed by the Zimbabwe Anti-Corruption Commission (ZACC) and they have identified some malpractices in tendering processes which have exhibited some element of conflict of interest in which companies owned by employees were suppliers to the employer; bribery for business favours and awarding contracts and extortion mostly by security forces. Within the broad category of

asset misappropriation, employees deployed several tactics to steal funds and other resources from their employers. According to the Global Study on Occupational Fraud and Abuse (2020), billing schemes were the most frequent, common and costliest form of asset misappropriation. Billing schemes also caused a high median loss and of most significant risk. In descending order, cheque payment tampering and theft of noncash assets posed a significant risk and impact. Misappropriation of assets occurred when employees or third parties linked with a firm abused their power and authority to steal from the organisation through a variety of fraudulent practices. Asset theft occurred when a firm or a client's assets were used for personal advantage (Kassem, 2014). Insider fraud is another term for this. Cash and non-cash misappropriation were two types of insider fraud. Employees steal and profit from the company's assets, resulting in a breach of trust between them and their employer. When motive, opportunity, and rationalization are there, according to Wright (2010), commercial organizations were vulnerable to employee misappropriation. Employers should take the initiative to develop a work-friendly environment. Employees were motivated to conduct occupational fraud by an unfavourable work environment caused by employer negligence and financial limitations.

Fraudulent financial reporting is another form of occupational fraud that was associated with a poor working environment. Employees' purposeful overstatement or understatement of balances in financial statements is referred to as fraudulent financial reporting. Accounting procedures are typically judgemental, this sort of occupational fraud is often hidden and difficult to detect, resulting in a tight line between optimistic but acceptable financial reporting and fraud (ICAEW's Audit and Assurance Faculty, 2020). Although financial reporting fraud was the least common type of fraud, it resulted in the highest median loss for businesses, according to the Association of Certified Fraud Examiners (ACFE) (2019). Financial reporting fraud differed from asset misappropriation in that it was more difficult to detect. The latter was more widespread, but it involved smaller amounts of money, such as stealing items through trickery or committing billing fraud for personal gain. The former, on the other hand, may have not resulted in any direct financial benefit. Individuals may be driven to meet performance targets and associated indirect rewards, such as avoiding the loss of a bonus payment or an increased share price, by internal or external organizational pressures. Personal incentives, market pressures, a lack of ethics, deliberate compliance with financial analyst estimates, and attempts to influence the stock price all contributed to

fraudulent financial reporting. However, external audits, rules, and an independent board of directors are all proposed counter to prevent fraudulent reporting. With fair financial reporting culture, on the other hand, required as an ethical business culture.

2.13.2 External Insurance Fraud

External insurance fraud, unlike internal insurance fraud, is perpetrated by third-party service providers or external stakeholders such as claimants, with the exclusion of employees (IPC, 2020). External insurance fraud included providing false statements as well as fraudulent claims of the policyholder, such as consumer fraud, counterfeit documents in the purchase of an insurance policy, or claim-making through fraudulent coverage or payment (Yusuf, 2010). Intermediary fraud though a separate type of insurance fraud, but it's an extension of external fraud, fraud committed by independent insurance agents against insurers or policyholders (IAIS, 2007). The nature of external insurance fraud has continuously changed due to advances in technology that made it easy for identity theft and computer hacking. Identity theft in micro insurance has come in the form of synthetic identity. Synthetic identity theft occurred when organised crime syndicates pair a legitimate identity number, employment code (EC) number and or social security number with fake personal information, such as a name, birth date, and address. The syndicates then used the synthetic identity for various insurance fraud crimes. While hacking, that is, illegal entering into private companies, government departments and entities that usually contain information of a security nature such as names, identity numbers, the status of claims, bank accounts including the amount in banks, organised crime syndicates, have manipulated this information to their advantage (Central Intelligence Agency, 2018). Recent findings by the Insurance and Pension Commission (2020) showed that people from outside the insurance company planned and executed external fraud. The most sophisticated fraudsters targeted businesses by impersonating a business partner such as false supplier or false customer, or even a manager, all in order to collect counterfeit dollars or commodities. Identity theft, impersonation of voice and signature, persuasion, intimidation, fraudulent emails, and system infiltration were all techniques utilised by these emerging organised crime syndicates.

2.13.3 Intermediary Insurance Fraud

Insurance intermediaries assist in the procurement of insurance services and provide services to both insurance companies and individuals that meet the insurance coverage requirements. In the past, insurance agents and brokers were the two types of middlemen. The difference

between the two comes down to how they conducted business. Insurance agents usually had licenses that allowed them to work on behalf of the insurance company. The agents worked on behalf of the insurance company and are bound by the agency and insurance agreements (Arunga, 2012). The agency may be authorised to collect premiums and issue documents on behalf of the insurance company, according to the terms and circumstances of the agency agreement. Some insurance agents offered additional after-sales assistance to their clients in the event that they needed to file a claim with their insurance company. Insurance brokers, on the other hand, are full-time professional intermediaries who, after being licensed by the Insurance and Pension Commission, act on behalf of potential policyholders (IPC). Insurance brokers act on behalf of their clients, though they work under the instruction of their clients, they represent their clients in obtaining insurance coverage, advice and negotiating between the client and insurance service provider or insurance companies. As for after-sales services, brokers also represent their clients during the claims process. Brokers are usually paid a broker fee by an insurance company and a service fee by their clients. The International Association of Insurance Managers (2017) reported on detecting and preventing insurance fraud emphasising that the insurance intermediary performs largely independently and their service is important for the distribution, registration and filing of claims. As a result, they are important stakeholders who are involved in some of the most important processes and insurance exchanges, as well as in insurance risk management and fraud, as they receive, operate, and maintain client records, putting them in a position of trust between policyholders or clients and insurance service providers (Vaughan, 1997). Insurance intermediaries, on the other hand, have a history of abusing trust, as evidenced by cases of withholding premiums from policyholders until a claim is reported, insuring non-existent policyholders while paying a first premium, collecting commission, and then cancelling the insurance by ceasing further premium payments, and colluding with policyholders to commit claims fraud or other types of fraud, such as backdating transcribed documents. Insurance firms are responsible for putting in place security measures and taking all reasonable means to ensure that intermediaries follow the terms and conditions of the agreement and satisfy defined criteria in order to appropriately preserve sound business practices. Insurers should only give business to security cleared intermediaries to achieve this successfully (President's Department, 2018).

2.13.4 Opportunist Fraud

In the strictest sense, opportunistic fraud is not a distinct sort of fraud. Opportunistic fraud can be conducted on any sort of insurance, from personal injury claims in automotive or commercial liability to property, pet, or travel insurance and beyond and by anyone with an opportunity to do so (IPC, 2020). Opportunistic fraud involved a person or an organised group of people conniving to submit a bogus claim on a single or several occasions. People or an organised group of people even those who have never committed a crime before will see a chance to cheat their insurance company, perhaps through a valid claim. Opportunistic fraud can be committed on all types of insurance. Organised criminal syndicates have taken advantage of the current worldwide corona virus (Covid-19) health situation causing widespread anxiety and a lot of misinformation, rumours and speculation. Dr Charles Mok, the creator of American Allure Medical, is a notable case of opportunistic fraud, since he was arrested for billing insurers for Vitamin-C infusions illegally portrayed as COVID-19 treatments and prophylactic measures during the COVID-19 pandemic (Hall, 2020).

2.13.5 Syndicate Fraud

Australian Organised Crime and Intelligence Group (2017) defined syndicate fraud as an organised criminal act conducted by syndicates or organised groups that target and penetrate insurance companies and policyholder, most commonly for profit. With a combination of economic downturn and lack of technological advances in Zimbabwe, insurers have become under increased threat from organised insurance fraud which costed the insurance industry more than three hundred and forty million United States of America dollars per year (Minister of Finance and Economic Development Ncube, 2020). Findings by the Ministry of Finance and Economic Development (2020) have indicated that organised insurance fraud is not only targeted at insurance companies offering services to low-income earners but to individuals such as the retired, elderly, students and other vulnerable people as well who are either policy holders or potential. Organised crime groups are increasingly being involved in insurance fraud and this is a recent development in organised insurance fraud. Money market diversifications, greater need for insurance services, general economic activity and technological developments have created opportunities for organised insurance fraud (Australian Criminal Intelligence Commission, 2019). There is consistent and widespread concern across the insurance industry and security sector about the negative impacts that organised insurance crime has upon the security of individual citizens, communities,

businesses and the insurance industry in general. Preliminary studies conducted by the Coalition against Insurance Fraud (2017) revealed that insurance fraud was being peddled by organised crime rings and has become part of a modern global crime nexus. Organised criminal syndicates in different countries are taking advantage of globalisation that has changed global trading to online trading thereby; this has allowed money transaction systems to fluidly move goods, services and commerce throughout the global economy and across international borders. Covert investigation conducted by the Zimbabwe Joint Operations Command (2019) revealed that organised crime syndicates no longer operate in isolation, but they recruit sources and contacts within targeted insurance companies, in some cases, they connive with policyholders. This has however, increased their success rate and reduced chances of detection.

2.14 State of Security Countermeasures in the Micro Insurance Sector

In the micro insurance market, insurance fraud has been a threat that necessitated an integrated counter measure approach at all levels, government, insurance companies, policy holders and the insurance industry all included. Given the numerous challenges that have hampered the development of micro insurance in Zimbabwe, the security intelligence, insurance experts and professionals suggested that the departing point to counter insurance fraud is an examination and understanding of the current state of insurance fraud countermeasures deployed by insurance companies. This was against the backdrop that an understanding of the current system will inform the designing of innovative state-centric, systems and artificial intelligence countermeasures. In Zimbabwe, since year 2000 mobile technology has revolutionised the financial service sector which has also enabled micro insurance to be remotely distributed across the world. This mobile technology through mobile money and e-wallet opened up new channels for insurance distribution and insurance claims even for the unbanked population (Technology in Micro Insurance, 2019). The failed initiative by insurance companies to employ advanced proactive controls designed to detect potential fraudsters during and after the applications process was a leading concern. Though there are various artificial intelligence systems, applications and software ready for deployment by insurance companies in the micro insurance market, micro insurance service providers has exhibited laxity in investing in such technology that could possibly detect, minimise and counter insurance fraud. Counter measures available for insurance companies included referencing applicant details against insurance industrywide

watch lists usually maintained by the insurance and pensions commission and security intelligence apparatus. Profiles and criminal activities of organised crime syndicates are monitored, maintained and regularly updated in the security intelligence databases. The database is accessible upon request and clearance by the National Intelligence Director General. Liaison with national intelligence apparatus have assisted other insurance companies to generate their own internal watch list and this could go a long way in assisting micro insurance companies in initially identifying known fraudsters at the policy application phase hence this become the first line of defence (Insurance Fraud in the Digital Age, 2017).

Extensive 'rules-based analysis' was also identified as an application to spot, identify possible fraudulent applications as well as false claims made by successful candidates post successful insurance application and acceptance. Data technology, on the other hand, was a technology to lower the risk of insurance fraud. This technology provided new capabilities to collect, acquire, and analyse data that was useful to insurance companies. To date, there is a plethora of new technological capabilities for collecting customer data in real time in an automated and non-intrusive manner and this technology has capacitated insurance companies to better identify insurance fraud risks (Institute of Internal Finance, 2016). Zimbabwe is noted excluded from global insurance fraud threats and counter measures (Insurance and Pension Commission, 2018). A study of societal participation in suppressing insurance fraud revealed that individuals within a society and third parties feared to assist the police and law enforcement personnel during the investigation process. Further, the ability of law enforcement agencies, the insurance industry, and insurance firms to investigate fraud was also being harmed by data privacy laws and other related legislation (Global Claims Fraud Survey, 2017). The issues facing the insurance sector and insurance companies around the world in combating insurance fraud are tabled in Table 2.2 below.

Table 2.2: Claims fraud survey

AMERICA	EUROPE, MIDDLE EAST AND AFRICA	ASIA
----------------	---------------------------------------	-------------

<ul style="list-style-type: none"> ▪ Lack of resources. ▪ Lack of analytical tools to detect fraud ▪ Difficulty obtaining evidence ▪ Questions/forms for family members after the death of a loved one 	<ul style="list-style-type: none"> ▪ Lack of support from legal authorities. ▪ Personal data protection laws. ▪ Sales process agency rules. ▪ Resistance from agency, claimant, doctors, etc. cooperating with the investigation. ▪ Politicization of the insurance industry. ▪ Poor internal control systems. ▪ Lack of artificial intelligence systems. ▪ Lack of intelligence sharing. ▪ Lack of resources. 	<ul style="list-style-type: none"> ▪ Resources and cost. ▪ Resistance from agency claimant, doctors, etc. cooperating with the investigation. ▪ Difficulty obtaining evidence. ▪ Absence of insurance repository enabling easy insurance shopping for smaller insurance amounts. ▪ Lack of analytical tools to detect fraud
--	---	--

(Source: Global Claims Fraud Survey, 2017)

2.15 Insurance Regulation

The Insurance and Pension Commission oversees insurance regulation in Zimbabwe. The Insurance Act of 1987 governs the provision of life and non-life insurance services in Zimbabwe, and the National Pension Scheme (NPS), Workers Compensation Insurance Fund Scheme (WCIF), and third-party liability insurance for motor vehicles are also required. The Zimbabwean government authorized one hundred per cent of direct foreign investment (FDI) in Zimbabwe's insurance sector. In the regard, the Zimbabwean insurance sector does not, however, permit the use of middlemen or insurance businesses that have not been admitted by the insurance and pension commission. The Zimbabwean insurance industry is a unique one and over years has been mired with controversy and corruption. Policy holders supported by several individual members of the public, as well as insurance and pensions representing organisations in the year 2015 lodged numerous complaints which prompted a commission of inquiry to be established by the Government of Zimbabwe in 2017. During the year 2008, the government of Zimbabwe entered into a Government of National Unity (GNU), proposed the

adoption of the United States of America dollar as the leading currency. This informed the conversion of various services from the Zimbabwean Dollar (ZD) to the USA dollar including insurance, pensions and their values. The 2017 commission of inquiry was tasked to evaluate the impact of this conversion on insurance and pension values. The then major concerns were on the depreciation or loss of values on already contributed pension arrears, lost value owing to hyperinflation, intergenerational transfer of benefits, dollarisation conversions, compulsory complete pension commutations, loss due to demutualization of First and Old Mutual and conversion of pension schemes from defined benefit to defined contribution funds. This resulted in pensions going unfunded and one third outstanding lump sum for retired civil servants particularly members who saved in the army and police force. Further, conscious postponement of monthly pension's pay-outs and related dependent benefits and retirees from church-related hospitals and mission schools not being able to access pensions were among the complaints levelled against the Zimbabwe insurance system. In addition, criticisms about the National Social Security Authority (NSSA) focused on the issue of arbitrary and consistent benefit calculations, National Social Security Authority (NSSA) pensions had become difficult to be accessed by civil servant, tertiary institutions students on attachment going without any form of insurance and poor record-keeping were all examples of National Social Security Authority (NSSA) constraints for claiming pension benefits. Other widespread complaints included failures by banks to process checks or even bank transfers issues by the National Social Security Authority (NSSA) and other insurance related services with bank transfers from micro insurance service providers not recognised by banks and health facilities. Further to this a plethora of malpractice issues were raised such as discontinuation of the issuance of employer contributions for retrenched employees, frequent changes in pension fund administrators resulting in the loss of contribution records, funeral assurance companies reneging on fully paid funeral covers when the economy dollarized, and absence of a Pensions Ombudsman.

Given the foregoing, it is strongly suggested that pension and insurance legislation be revised to allow the Insurance and Pension Commission (IPEC) to regulate permissible spending categories and ratios through regulations. The objective was to contain the widespread problem of unreasonably high expense ratios, ratios which exceeded one hundred per cent (100%) of the pension contributions or insurance premiums.

Furthermore, the importance of defining allowed expenses or charges, as well as their levels, were emphasised in addition to the requirement for minimum expense charges. The relationship between the Insurance and Pension Commission (IPEC) and insurance service providers in the industry was taken into account as well as the policyholder's premiums or contributions, and the expected advantages. The Insurance and Pension Commission (IPEC), in this case the regulator was granted the authority to make declarations. If the premium-to-premium connection was unsound, the product was also financially unsound. The downside was that it could result in a loss of faith in the insurance sector. Hence the regulator was empowered to impose procedures for monitoring and comparing the predicted benefits to the insurance and pensions premiums. A ruling by the Government of Zimbabwe was that the insurance industry was not de-monetised from the Zimbabwe dollar to United States of America dollars at the time of dollarisation and, as a result, Insurance and Pension Commission (IPEC) did not guide or approved the conversion of insurance and pension liabilities to ensure equity and fairness, but rather insurance industry acted in isolation. Furthermore, in the majority of cases, pensioners who got lump-sum pay outs in 2008 were unable to access their cash and were only able to collect five USA dollars due to the de-monetisation process. Insurance and Pension Commission failed to protect policyholders' rights and reasonable benefit expectations, such as mandating indexation of premiums and contributions, as well as pension increases to deter commutations of pensions in payment and guide the market during conversion, coasted policyholders and pension fund members' money.

There was no resolution process in place or statutory instrument for problematic insurance and pension institutions that needed to be rescued or liquidated. As a result, when the pension fund or insurance companies were liquidated, the assets of the pension and policyholders were divided to creditors of the pension fund or insurance company excluding policy holders. Insurance companies offering life insurance services whose licenses were revoked by the Insurance and Pension Commission lost their whole investment in the collapsed organization since there was no policyholder protection fund, prudential controls, or market conduct regulation; hence, policy holders also lost their savings. Furthermore, in the absence of regulatory direction, most conversions were done in a highly subjective and faulty manner that primarily safeguarded the interests of insurance companies at the expense of contributing policyholders. As a result, the values of policyholders were transferred to insurance company

stockholders. An audit by the Insurance and Pension Commission (2019) unearthed that the insurance industry as a whole, regulated and unregulated institutions, had major record-keeping issues. Evidently and deliberately, owing to poor record keeping, some insurance companies failed to provide accurate information to the Insurance and Pension Commission, information on accumulations of contributions and premiums for individual policy holders, investment returns, asset build-up, and copies of statutory returns over the investigation period. Policy holders claimed that losses to their contributions were also attributed to unscrupulous business entities, poor corporate governance procedures, including inappropriately constituted boards of directors and trustees, unskilled employees, conflicted boards of directors and trustees, and lack of technology and poor internal control systems, hence contributing to high level of insurance fraud. Two major causes of value loss were identified as excessive administrative and other expenses at the institutional level and insurance fraud. Industry expenses and insurance fraud, excluding benefits payments, accounted for eighty-one per cent of total premiums and contributions loss after dollarisation, leaving only nineteen per cent for investment.

In light of the above stated problems facing the Zimbabwe insurance industry, the National Association of Insurance Commissioners of United States of America (2019) referred to insurance regulation as that part of state regulation that protects consumers by ensuring that insurance companies irrespective of the type of service they offer, meet their contractual obligation through various requirements such as insurer licensing, broker licensing, insurance policy regulation, financial regulation, market conduct, and consumer protection services. The prescribed ideal situation was that, the government should regulate insurance companies and the insurance industry as a whole. This can only be achieved by recommending and passing state laws, statutory instruments, directives, statutes and standards that should guide the conduct of the insurance industry and operations of individual insurance companies. The Insurance and Pension Commission has regulated insurance in Zimbabwe under the Insurance Act 27/1988, 19/98 (s. 14), 22/2001 (s. 4), and 3/2004. The acts were enacted in 1988, but have however been amended several times between year 2001 and 2004. The state played a pivotal role in the amendments and according to the Insurance Act of Zimbabwe, the term "state" referred to situations in which the government enacts an enabling Act of Parliament that establishes a statutory agent or authority to control a certain sector.

The Insurance and Pension Commission Act of 2000 Chapter 24, by act of parliament established the Insurance and Pensions Commission (IPEC). The Insurance and Pensions Commission (IPEC) carries out its responsibilities under the Insurance Act 24 and the Pensions and Provident Fund Act 24: The Insurance and Pension Commission has also enacted subsidiary legislation through Minister of Finance and Economic Development to complement the existing legislation while the Commissioner of Insurance and Pensions Commission has also issued guidelines, circulars, or directives to standardise the insurance industry. In light of the foregoing government of Zimbabwe authorised authorities such as the Insurance and Pension Commission are empowered to oversee insurance companies' solvency, market conduct, reviewing and ruling on petitions for coverage rate increases. In this regard, any person, entities which engages in any class of insurance business in Zimbabwe was directed to first apply to the Insurance and Pension Commission, followed by being inspected and registered by the regulatory authority as an insurance entity in the applied category of insurance business. One of the most important prerequisite for an entity to be granted an operating license was a criminal police clearance of the directors of the company. Insurance companies who operated without authorisation and licence from the Insurance and Pension Commission were charged with a criminal fine of level fourteen or ten years' jail sentence, or both. Rejda (2009) argued that court judgments also played a pivotal role in regulating the insurance industry, court judgements were significant as they examined the constitutionality of insurance legislation, interpretation of insurance contracts, and the legality of actions of the state regulatory agency thus shaping the entire industry. The insurance industry also voluntarily agreed with the government in memoranda of agreements to implement mutually agreed professional best ethics, practice and standards.

It is pivotal to highlight that National Association of Insurance Commissioners (NAIC), (2015) also prescribed some mutually agreed standards for the insurance industry. Members of the NAIC with diversified experiences, political perspectives, and geographic locations, but all committed to protect insurance policy holders and ensuring fair, competitive, and health insurance have since assisted insurance regulators in safeguarding the insurance industry and protecting policy holders' customers by creating standards, conducting peer reviews, and coordinating regulatory oversight. Gordon (2021) mentioned that the National Association of Insurance Commissioners, in collaboration with its members, has provided to

various states a nationwide structure of government oriented insurance regulations particularly common financial reporting requirements for insurance businesses. The NAIC capacitated insurance regulators in serving the public interest and attaining certain essential regulatory goals, both individually as singular insurance company and collectively as an industry. According to the Insurance and Pension Commission Board Chairperson, Nduna (2020), the insurance industry in Zimbabwe should emulate the recommendation by the Association of Insurance Commissioners (NAIC) since they also aid in countering insurance fraud. Nduna (2020) further confirmed that insurance fraud is not only a threat to the insurance industry but the nation as a whole. Government, scholars, law enforcement agents and intelligence officers in Zimbabwe through inter-agency communication and information collaboration agreed that the insurance industry and insurance companies in Zimbabwe and around the world should be regulated to protect policy holders in society, but also categorically expressed the need to seriously regulate micro insurance service providers since they cover a substantial vulnerable population in any given country. Given that insurance policies are optional, but a general trend in Zimbabwe is that low income earners were highly encouraged to make use of micro insurance as an effective social protection net. In that vein, contracts drafted by insurance companies are also known as contracts of adhesion, this magnified the pivotal role that insurance regulators must play in protecting and promoting policyholder interests throughout the existence and demise of insurance companies. Various opinions have been forward with regards to the importance of insurance regulations which has been commended also as a tool to counter insurance fraud, it has encouraged the uptake of insurance by low income earners and also has complemented government developments initiatives and economic stability. The Zimbabwe Ministry of Finance and Economic Development (2020) cited six (6) various reasons with example from across the globe why insurance should be regulated and these were:

- i. **To address market irrationality by insurance companies and members of the public:** Pfister (2014) reported that insurance experts and various professionals in micro insurance concur that micro insurance is a rapidly expanding area that required serious, air tight regulation. New micro insurance companies have been formed and microfinance institutions have included insurance services in their product offerings targeting low income earners as their client base. Low-income earners through advertisement and insurance awareness campaigns have been enlightened of micro

insurance and the demand has since been overwhelming. Insurance experts, insurance companies, governments, political structures and non-governmental organisations (NGOs) all have viewed micro insurance as a way to reduce structural poverty. Experts concur that without this growth, expanding demand for micro insurance, this new industry will expand slowly and, worse, its long-term viability may be jeopardised due to rampant insurance fraud cases worse if it goes unregulated. Micro insurance regulation or its lack thereof has distinct effects on different categories of stakeholders within the industry. Regulations specify insurance company operational criteria, give consumer protection through insurer oversight to ensure their solvency, and protect customers from purchasing insurance from unsuitable or even unregistered insurance companies.

- ii. **Market failures and biased precedents are both harmful to society:** According to economists Vernon and Harrington (2000), the occurrence of market failures, such as economic crises, supports regulation of the insurance industry. The economic downturn in Zimbabwe is one example in which the economic collapse eroded all insurance related savings. Zimbabwe's economy has been afflicted by a number of monetary and fiscal challenges, particularly inflation, deindustrialisation, high borrowing interest rates and liquidity shortages (Mpofu, 2015). The Government of Zimbabwe due to economic meltdown adopted a multicurrency regime in 2008 in a bid to arrest and address the economic crisis (Reserve Bank of Zimbabwe, 2016). The term 'dollarisation' became common to describe Zimbabwe's multicurrency regime for two reasons. The difficulty was that, as of 2019, the Zimbabwean economy was still weak, with high inflation, tight liquidity, high-interest rates, unsustainable external liabilities, massive de-industrialisation, and formalisation. The Reserve Bank of Zimbabwe (RBZ) (2018) attributed most of the country's economic stagnation to liquidity issues caused by dollarisation. As a result, dollarisation posed several difficulties. It deprived the country's monetary policy autonomy, effectively reduced the central bank's role to that of a regulator. Several enterprises across a variety of industries, including those in the insurance industry, closed as a result of economic concerns. Between 2009 and July 2017, a total of forty-two (42) insurance companies in Zimbabwe were closed due to dollarisation, with twenty-one (21) being brokers, thirteen (13) being non-life insurance companies, three (3) being life insurance companies, three (3) being reinsurers, and two (2) being funeral assurance companies.

According to Machinjika (2018), insurance regulation safeguarded the financial viability of insurance businesses by requiring solvency counter mechanisms, risk limitation, qualifications, performance, disclosure, reserves, reporting (periodicity, accounting, and information systems), auditing, and investment constraints. According to the United Nations Conference on Trade and Development (1994), the established public confidence in entities which make up the finance and insurance sectors, as well as political and economic stability, is a prerequisite for developing robust financial entities, which are one of the pillars of modern society. Trust can only be maintained if these organizations keep their commitments. The government is therefore seized with an objective to foster and provide an environment that ensures continued stability and dependability of the financial system's components.

- iii. **To make up for a lack of insurance consumer information:** In any contractual connection between the policy holder and the insurer, the information available to both parties is asymmetrical. It is difficult for the insurance company to gather information about the insured and monitor the insured's behaviour once the insurance contract was signed. Those who wanted to insure themselves were more inclined to take greater risks than the uninsured general public. This implied that the insured may be less cautious than those who are not. These are referred to as adverse selection and moral hazard problems, respectively (The Spanish Economy monthly report, 2012). Insurance contracts, according to Rejda (2011), are legal documents with extensive terms, conditions, warranties, and provisions. There is a large information asymmetry in favour of insurance companies, which may propose overly restrictive and legalistic policies to society's detriment. There is a need to protect the public from unscrupulous agents and brokers who may mislead by promising loans if they purchase insurance. These informational issues were the standard reason for regulation. The regulation aimed at addressing information issues that could be solved by the market alone. In the private sector, information challenges experienced by businesses were usually resolved rather quickly. Employing business practices for exclusions or overpricing some groups who are more likely to take excessive risks, for example, and consumer-related issues virtually always required government oversight.
- iv. **To address supply side challenges:** In India, the Insurance Regulatory and Development Authority (IRDA) required life insurers to hold at least nine per cent (9%) of all policies to be rural insurance. This was a move meant to advance micro

insurance to low income earners and any resistance attracted penalties thereby ensuring financial inclusion-micro insurance. In today's market, risk insurance is a multi-faceted endeavour. People all around the world have been afflicted by a viral disease outbreak caused by the new coronavirus since 2019. The World Health Organization (WHO) has proclaimed the 2019 corona various (COVID 19) disease a pandemic. According to the World Health Organisation (WHO) (2020), more than two hundred and thirty-one (231) million cases had been confirmed as of September 2021, with over four hundred and seventy-three (473) million recorded death cases attributed to the corona virus(COVID-19), making it one of the worst pandemics in human history. Inadequate raw materials, rigid production lines, and stalled logistics began to impede the delivery of critical lifesaving goods and services to the market, forcing businesses, particularly insurance companies, to struggle to meet their medical orders. Hoarding hindered the restricted amounts of key commodities and services from being distributed equitably to consumers, even while supply was already below market demand. Panic purchasers stockpiled medical and non-medical items as long as they are readily available and reasonably priced. This illogical behaviour destabilised the market and worsened shortages situation across the globe (Price, 2020). On the other hand, service providers took advantage of the chance to raise prices to increase earnings. Since the beginning of the pandemic, the price of surgical masks has escalated six fold, the price of N95 respirators has trebled, and the price of surgical gowns has doubled, according to the World Health Organization (WHO) (2020). Government involvement was required in this form of market distortion. When creating regulations for a global pandemic, policymakers must examine supply networks influenced by both the supply and demand sides, which is a challenging task. To date, Zimbabwe's government has concentrated its efforts on supply-side pricing and service provision, such as insurance, as well as demand-side purchasing control, such as limiting customer demand.

- v. **Fostering public safety on innocent third parties and society at large:** According to the Insurance and Pension Commission (IPEC) (2020) insurance has been recognised as a vital tool for managing risk in the modern world, a tool that was also identified as an innovative social safety net for low income earners. Insurance has enabled both the commercial sector to mitigate risk while individuals were positioned to better manage future uncertainty. The ratio of aggregated insurance premiums (life

and non-life premiums) to gross domestic product in several developed countries exceeded ten per cent (10%), demonstrating the insurance industry's economic importance. The policy holder buys a future promise of payment depending on the occurrence of specified events, which is the core feature of a non-life insurance contract. This meant that the policyholder pays first, and then the insurer may be forced to reimburse the insured or a third party for a claim at some point in the future. This has had a number of implications, including the need for an insurer's long-term reliability to be established; and money entrusted to insurers, which are used to fulfil future liabilities in major part. Though there may be an imbalance in the contractual relationship between the insurance company and the insured, policyholders are however, protected. It is worth noting that original insurance regulations were established to protect insurers from fraudulent behaviour on the side of the insured such as over insurance, and multiple insurances. Only around the turn of the twentieth century, with the introduction of compulsory insurance which included motor, liability, and occupational compensation in some countries, and the increasing complexity of insurance contracts, legislators begin to be more concerned with protecting the interests of policy holders and third parties. With the emergence of "consumerism" following World War II, this trend escalated. Most new insurance related regulations cited the public's protection and fair treatment as a significant issue. Consumer protection legislation in several nations has also evolved beyond concerns about seriousness and honesty offer insurance cover, other factors such as policy price, and quality of insurance services offered, flexibility and availability. The General Agreement on Trade in Services (GATS), which was finalised as part of the Uruguay Round negotiations, stated that member countries "shall not be prevented from taking prudential measures, which included protection of policyholders or to ensure the integrity and stability of the financial system" in the case of financial services. That was amongst the reasons why the insurance industry should be regulated. The head of Insurance and Micro Insurance at the Insurance and Pension Commission, Machinjika (2018) mentioned that the existence of market failures as precedents of prejudice against society. Market failures, such as economic crises, are cited by Vernon and Harrington (2000) as justifications for regulation. In the period from 2009 to July 2017, a total of forty-two (42) insurance companies in

Zimbabwe were closed due to dollarisation. These insurance businesses' closures resulted in the immediate termination of insurance services for their policyholders.

- vi. **Insurance funds can be applied in developmental initiatives:** Insurers have large sums of money that are invested to generate further profits. These funds are even developing other industries not related to insurance. Insurance companies which have exhibited the need to be competitive and continue serving the market have applied the excessive revenue in the insurance service delivery and resultantly, the insurance companies have been offering cost effective insurance policies to its clients. As a result, the administration of these funds is crucial for insurers and policyholders, as well as having a significant impact on the national economy. Appropriate legislation directing these funds to certain economic growth areas could aid the country's overall economic development. This issue has arisen regularly in the less economically developed economies, where financial capital for economic growth and development is typically scarce and wealth retained by insurance companies may alternatively be applied in economic development. However, tight investment limitations have been suggested as making it more difficult for insurers to maintain the required levels of liquidity and security in their investment portfolios. As a result of such legislation, companies may be deprived of higher-returning investment opportunities.

Research identified several regulatory areas that could be changed to make micro insurance more accessible to low-income earners in Zimbabwe. Regulation, or the absence thereof, has had diversified effects on micro insurance service providers. Traditional insurance regulations were created with organisations servicing the middle and upper-income groups as their target market taking into account their capabilities to service their policies by continuously paying premiums. As a result, these insurance restrictions unintentionally restricted insurance coverage for low-income earners and households. It was recommended necessary to change the regulations so that low-income individuals and households can get microinsurance services. Given the tiny number of policies, most minimum capital requirements are unnecessarily high, especially for locally organised small micro insurance organizations. Capital requirements assisted insurers in maintaining financial stability. Regulators usually demand high capital requirements, but this discourages established insurers from providing services to low-income earner and households who have limited policy amounts and contributions. Large insurance firms have been hesitant to enter this

sector because they fear the amount of business will not generate sufficient profit. Governments have tightened minimum capital requirements in some cases, such as Bolivia, forcing Crucea, a sustainable low-income insurance provider, to suspend operations. In some circumstances, the qualifications for agents were either too lax, allowing anyone to function as an agent without any prior training, registration and authorisation. Insurance legislation has since put serious prerequisites and in most cases several years of experience and practice is required along with industry based education, making it difficult for small and newly founded businesses to function as agents. Alternatively, the legislation promulgated that the identified agent be a real person, not a Non-Governmental Organisation (NGO). The latter and the exclusive business line of microfinance institutions frequently restricted them from serving as an agent. Policy details regulations also limited access to insurance markets that were dominated by low income earners. Low income earners were generally a group of potential policy holders, who are illiterate and unfamiliar with these procedures, struggles to comprehend lengthy insurance contracts written in legalese. Simple contracts and imaginative, pro-poor public communication campaigns were critical for micro insurance to overcome this problem. Conventional insurance regulations did not apply to semi-formal insurance programs. Semi-formal programs provided micro insurance while avoiding rules. As a result, their institutions and customers were both at risk. For generations in many countries, semi-formal and informal insurance plans have been a part of community life. Small schemes have continued to be important because they are usually the only source of insurance services because large commercial insurers avoided such market. Their financial soundness was a reason for concern, notwithstanding the fact that they were not prudentially regulated and overseen. Whether as agents or providers, these schemes should be conceptually incorporated into the formal financial system. However, not every semi-formal or informal insurance provider was required to be included in the formal financial system. There were few community-based systems for which the government was unable to take responsibility.

2.15.1 The Insurance and Pension Commission

As part of the insurance industry regulatory push, the Zimbabwean government enacted the insurance and pension's commission amendment bill, the insurance bill and the pension's provident fund amendment bill all targeted at the monitoring and regulation of both pensions and insurance entities and industries. The Insurance and Pension Commission (IPEC) on

establishment was controlled by a Board of Directors comprised of two (2) government employees or civil employees and any other five (5) individuals with the prerequisite background chosen for three-year terms by the Minister of Finance and Economic Development. The Commission was primarily funded by fees on the insurance and pension industries, which was imposed with the Minister of Finance and Economic Development approval. On September 10th, 2018, the Insurance and Pensions Commission Amendment Bill was published, gazetted. The Insurance and Pensions Commission was established under the Act to oversee the insurance industry in Zimbabwe. The Commission's responsibilities were recommended as follows:

- 1) Insurance firms, mutual insurance societies, insurance brokers, pension and provident funds must all be registered and regulated.
- 2) To keep the general public up to date on the insurance and pension industries, and
- 3) To provide industry advice to the Minister responsible.

In addition to the functions, the act had three goals. To begin, a fair, secure, and stable insurance and pensions system was to be established. Secondly, operational independence, accountability, and transparency were all required. Thirdly, to adhere to high professional standards, to be met by the industry rather than the Commission. Overlay, the insurance and pension commission had an autonomous goal of encouraging the industry to maintain a high level of confidentiality.

2.15.2 The board of the Insurance and Pension Commission's (IPEC)

The insurance and pension's commission amendment bill made several changes to the Insurance and Pension Commission's (IPEC) board and procedures to its functions. Clause five (5) of the insurance and pension's commission amendment bill prescribed operations of the Insurance and Pension Commission (IPEC) to be overseen by a board of directors. The board of directors was to be composed of five to seven (5-7) members. The board members were to be chosen for their experience in actuarial practice, law, finance, human resources management, information technology and related fields. As a corporate governance issue, clause six (6) of the insurance and pension's commission amendment bill disqualified any selected persons from membership of the board if they were employed or connected with an insurance company or other entity regulated by the Insurance and Pension Commission. The selected and appointed member were to serve the commission for a period not exceeding

eight (8) years, that is, two (2) four (4) year terms, on the Insurance and Pension Commission's (IPEC) board. A quorum of two to six members was required, authorised to compel the chairperson to hold a special meeting. In addition, the insurance and pension's commission amendment bill stipulated that the board had the authority to appoint committees to carry out specified functions that could be directed from time to time by the commission. Further, the bill required the board of directors to appoint at least two committees, according to clause nine (9) of the bill though surprisingly, it was silent on the roles, duties and function these committees.

2.15.4 Functions of the Insurance and Pension Commission's (IPEC)

The insurance and pension's commission amendment bill proposed to broaden the Commission's responsibilities to include accrediting actuaries, auditors, asset managers, credit rating agencies, and "other service providers in the insurance market," according to clause four (4). However, the act did not provide the Commission legal authority to compel actuaries, auditors, and other professionals to become accredited, nor did it specify how they should apply for accreditation or how long their accreditation would continue. This created loopholes in the regulatory role of the commission. The provision was useless without such authority. Under the Public Accountants and Auditors Act, the Law Society of Zimbabwe (2020) auditors were properly registered and regulated. The Asset Management Act also required asset managers to be registered and regulated. These professions previously did not require accreditation.

Clause eleven (11) of the insurance and pension's commission amendment bill authorised and empowered the Insurance and Pension Commission (IPEC) to consult, liaise and cooperate with other regulatory authorities, law enforcement agents and the security intelligence community both local and foreign, in such matters as enforcing laws, carrying out investigations and exchanging information. The Director General of the President's Department, Moyo (2022), opined that clause eleven (11) may be utilised by the Insurance and Pension Commission to deal with issues of corruption and fraud within the industry in consultation with external stakeholders such as the security intelligence community. This was a commendable clause because insurance businesses and pension funds operate beyond national borders, necessitating collaboration among regulatory bodies to ensure compliance with all applicable laws. However, there was one aspect that was emphasised considering the sensitivity and risk associated with intelligence sharing. The Commission was authorized to

request and receive "privileged information" from other authorities such as the national security intelligence apparatus, but was not be required, authorised to reveal the "privileged information" obtained from such authorities to third parties, according to clause eleven (11) of the insurance and pension's commission amendment bill. This was particularly important considering that exchanging security intelligence; its publication could be harmful to other parties, put at risk the lives of undercover officers and jeopardize on-going investigations and intelligence collection operations.

2.15.5 The Insurance Bill

The Insurance Bill of 2020 and 2021 proposed to abolish and replaced the Insurance Act [Chapter 24:07], which however received Cabinet approval due to loopholes in the previous bill. Lobbyists supporting the bill stated that amongst the several goals of the bill, it was important to implement best practices that have long been requested in the insurance business, contain or counter insurance fraud and improve policyholder protection. The bill suggested that insurance businesses followed best practices with solid corporate governance systems in place both at the company and industry levels. The bill aimed at improving insurance companies' internal control systems and good corporate governance by encouraging the use of international best practices in corporate governance. Some of the amendments to the Bill aimed at guaranteeing that the Insurance and Pension Commission (IPEC) was satisfied right from the start that the registered insurance companies operating in Zimbabwe have suitable management systems and are conducting their business responsibly and lawfully. The Bill provided civil sanctions to those found in breach by the Insurance and Pension Commission, demonstrating its commitment to enforcing good corporate governance. Mechanism to monitor and evaluate the insurance industry was also introduced with the bill; the bill proposed the appointment of detached, independent directors who would serves on the Board of Directors. It required independent directors to make up at least two-thirds (2/3) of a society's board of directors or other governing body. Furthermore, independent directors made up the majority of the audit committee. The audit committee's chair wasalso required to be one of the independent directors. Further to put checks and balances, the Bill included a new clause that governed the nomination, appointment, authority, and tenure of inspectors to improve insurer monitoring and investigations. It recommends that anyone can be appointed as inspector once the Insurance and Pension

Commission (IPEC) believed they have the relevant experience, qualifications, or skills to carry out stipulated duties as an inspector.

The insurance bill further recommended new methods of assessing the margin of solvency, it targeted specific important requirements to change from time to time, to minimise insurers insolvency. The following elements were considered most cases: the type of insurance, the asset-to-liability ratio, foreign currency liability, capital market movements, policyholder protection, and international best practices. The idea of resuscitating failed firms was borrowed from the Insolvency Act [Chapter 6:07]. It introduced the concept of curatorship under which the Insurance and Pension Commission (IPEC) may order an insurer to be placed under curatorship if it fails to fulfil minimum financial standards or fails to function following acceptable administrative and accounting processes. The bill also proposed to introduce micro insurance enterprises to provide insurable interest to low-income consumers. In terms of pricing, scope, coverage, and delivery mechanism, the micro insurance industry was geared toward providing insurance to low-income groups of the population. This niche provided low-income earners with particular protection against certain perils in exchange for recurring premium payments that were proportional to the likelihood and cost of the risks involved. With retrospective provisions on a currency conversion, the Bill strengthened the protection of policyholders even more. It stated that every insurer must have its actuary assess the insurer's liabilities in the previous currency to its policy owners and other stakeholders after the currency conversion date, which was June 24, 2019, taking into account the following:

- Investment returns up to that date;
- The policy premium up to that date;
- Premium payment period;
- Rate of inflation; and
- Other factors may be necessary

2.15.6 Pension and Provident Funds Bill [Chapter 24:09]

The Pensions and Provident Funds bill has been in force since 1976. Over time, the Insurance industry has seen dynamic changes financially and administratively without any major adaption by the governing act. As a result, calls for change based on the challenges within the Insurance and Pension sector were noted and, accordingly, a Commission of Inquiry into the Conversion of Insurance and Pension Values was established in terms of Statutory Instrument

8 of 2015. In that regard, insurance experts in Zimbabwe noted that, among other things, the major problems that had stormed the insurance industry were:

- The loss of value arising from pension contribution arrears;
- Loss of value due to hyperinflation;
- The loss of value through conversions and dollarisation;
- Delayed processing of lump sum pension benefits; and
- Poor policy formulation to govern the industry.

As far as regulatory efforts and novel ideas to address some of these challenges, the majority of recommendations focused on the need for a complete overhaul of the Insurance and Pension Commission (IPEC), overhaul or changes on policy, and the adoption of a comprehensive insurance scheme, as well as consumer protection and good governance. The Pension and Provident Funds bill [Chapter 24:09] (2019) repealed the Pension and Provident Funds Act and provided for the registration, regulation, and dissolution of pension and provident funds. The Pension and Provident Funds Bill specified that evidential value and validity duration of a certificate of registration in clause eleven (11), a certificate of registration of a fund shall, upon production and concrete evidence of the absence of insurance fraud cases and all registration requirements of the bill, with that the fund is duly registered. A certificate of registration issued to a fund shall be valid from the date of issue and shall remain in force until the fund is dissolved or the certificate of registration is revoked following procedures of the bill. Pension provision was critical in terms of both economic and social well-being, as it ensured appropriate retirement income delivery. The promise to pay a retirement benefit to today's workers included a period that could last decades. One of the most critical considerations in the design of retirement programs was the ability to keep these promises. As a regulatory body, the Insurance and Pension Commission (IPEC) had a right to administrative justice. The insurance and pension commission (IPEC) had a major role as the regulator of pension funds. Nonetheless, the bill provided that the insurance and pension commission (IPEC) will have to adhere to basic principles of corporate governance in carrying out its role. Its duties were discharged in a lawful, prompt, efficient, reasonable and proportionate way. Any failure on the part of the insurance and pension commission (IPEC) was subject to administrative review, especially with regard to the powers which the insurance and pension commission (IPEC) will have to revoke certificates of registration according to the breach of conditions or misrepresentation by a pension fund. The Pension

and Provident Funds Act's main goal was to ensure that policyholders and retirees are protected. One of the key goals of the bill was to ensure that customers are treated properly. This was to be achieved by, first, value preservation.

According to the bill, the board of every existing pension fund was directed that after a currency conversion date, cause the fund's actuary to calculate the fund's liabilities in the former currency towards the policy holders and related stakeholders at the currency conversion rate and date, and cause the fund's actuary to apportion the fair value of the fund's assets in the new currency between the members, beneficiaries, and other stakeholders to establish, as far as possible, the fund's liabilities in the former currency towards its Corporate governance issues were also discussed. The Pension and Provident Funds Act mandated that the pension fund be managed by a board of trustees. The board made up of members who are fit and proper to assure integrity. The Pension and Provident Funds Act promoted the use of digital technology to counter insurance fraud, reduce time and costs in the Pensions and Insurance industry and to bring it up to international standards. Critics argued that the law should be linked to the recently enacted Consumer Protection Act, whose principal goal was to safeguard policyholders and retirees.

2.15.7 The Zimbabwe Anti-Corruption Commission

To complement the already existing security apparatus in the insurance industry, the Government of Zimbabwe established the Zimbabwe Anti-Corruption Commission (ZACC) in addition to the regulatory authority and law enforcement agents. The Zimbabwe Anti-Corruption Commission (ZACC) a standalone commission created to counter corruption and fraud. Its duties and responsibilities are broad. It was formed under Zimbabwe's constitution, Chapter thirteen (13), part one (1). The first commissioners of the Zimbabwe Anti-Corruption Commission were sworn in by the President of Zimbabwe on September 18, 2015. This was after realisation that corruption in Zimbabwe was widely viewed as one of the most significant setbacks affecting various economic sectors and subsequently the economy. Corruption and fraud are frequent crimes across African countries, according to the Reserve Bank of Zimbabwe (RBZ) (2020), and the two are blamed for low economic growth, severe socio-economic inequality, and poverty. Since 1980, Zimbabwe has seen an increase in corruption and fraud, with proceeds from these crimes being channelled to fund other crimes such as terrorism and insurgency, resulting in a fast failing economy.

In view of the foregoing, Zimbabwe's government made initiatives to eradicate corruption. The Zimbabwe Anti-Corruption Commission's (ZACC) efforts revolved around anti-corruption. Its principal objective was to counter and contain corruption in the entire economic sectors. Further, the Zimbabwe Anti-Corruption Commission recommended research based corruption counter measures to the government and private sectors. The initiatives were meant to strengthen accountability, promote integrity, and prevent fraud. Zimbabwe is a signatory to a number of regional and international anti-corruption treaties, as well as anti-corruption constitutional provisions. The SADC Protocol against Corruption was signed in 2001 and ratified in 2003; the African Union Convention on Preventing and Combating Corruption (AU Convention) was signed in 2003 and ratified in 2006; and the United Nations Convention against Corruption (UNCAC) was signed in 2005 and ratified in 2007. The Zimbabwe Anti-Corruption Commission (ZACC) on establishment was tasked with the following functions in accordance to the lessons learned from several regional and international anti-corruption conventions:

- a) To investigate and expose public and commercial sector corruption;
- b) To fight against corruption, theft, misappropriation, abuses of power, and other unethical behaviour in both the public and commercial sectors.
- c) Encourage honesty, financial discipline, and openness in both the public and private sectors;
- d) Receiving and considering public complaints with regards to fraud and corruption, as well as taking necessary action in response to the complaints;
- e) To order the Commissioner-General of Police to examine cases of alleged corruption and report back to the Commission on the findings;
- f) To refer cases for prosecution to the National Prosecuting Authority;
- g) To help officers of the Police Service and other state-run investigating agencies; and
- h) To offer suggestions to the government and others on how to improve integrity and accountability in the public and private sectors, as well as how to prevent improper conduct.

Fighting insurance fraud since inception was a priority for both the insurance industry and the Insurance and Pension Commission (IPEC). It was therefore imperative for the insurance

industry, the Insurance and Pension Commission (IPEC), the intelligence community and law enforcement agents to share notes and collaborate with the Zimbabwe Anti-Corruption (ZACC) as well. Insurance fraud, considered a serious crime, with serious implications to the fraudsters such as criminal conviction, and incarceration.

Transparency International, the world's premier non-governmental anti-corruption group, defined corruption as "the abuse of entrusted power for private gain". Similar definition is referred and referenced on various scholarly literature on corruption. Corruption, for example, was defined by Ashforth and Anand as "the abuse of authority for personal, subunit, and/or organisational advantage". Bribery, extortion, embezzlement, theft, and fraud are examples of corrupt activities, the abuse of discretionary powers, favouritism, regulatory capture, nepotism, and clientelism. Corruption is recognised as a severe worldwide issue and a root cause of poverty, inequality, terrorism, and conflict. In the last decades, national regulators, international financial and policy organizations, corporations, campaigners, and the media have all been interested in the subject. The International Consortium of Investigative Journalists (ICIJ) has worked to reveal offshore financial arrangements that aid in corruption, prompting a re-examination of the role of the international financial system in supporting corruption, including "enablers" such as attorneys and accountants. Wathne and Stephenson (2021) highlighted that it was difficult to assess the true magnitude and cost of fraud; with fraud and corruption being one of the most difficult crimes to obtain evidence, hence the majority of commonly used numbers are flawed or wrong. Anti-corruption activities and strong insurance sector regulation are justified by the inherent immorality of corruption, as well as the well-documented risks or harm to individuals, organizations, and society.

A study by the anti-corruption unit within the President's department (2020) revealed that insurance companies and other companies in general have failed to eradicate corruption due to the pervasiveness of corrupt behaviours in business and lax legislations. As a result, at the recommendation of the Insurance and Pension Commission (IPEC), the security intelligence community and the Zimbabwe Anti-Corruption Commission (ZACC), the government of Zimbabwe needed to reconsider and come up with an air tight anti-corruption mechanism. An anti-corruption mechanism regarded legal defence against internal and external forms of corruption, a proactive measure in which the national security intelligence would counter the operations organised crime syndicates. Such mechanism has been implemented in the United Kingdom by the Ministry of Justice in 2010. The mechanism gives lengthy guidance on the

key aspects of anti-corruption programs, which are consistent across countries and include the following elements:

- Senior management commitment and a transparent anti-corruption strategy;
- Policies and processes for conformity with the code of conduct;
- Supervision, independence, and resources;
- Risk evaluation;
- Instruction and on-going guidance;
- Discipline as well as incentives;
- Payments due diligence for third parties;
- Internal investigation and secret reporting;
- Continuous improvement: reassessment and testing on a regular basis
- Mergers and acquisitions: pre-acquisition due diligence and post-acquisition integration; and
- Intelligence gathering and monitoring of known and potential organised crime syndicates.

The Zimbabwe Anti-Corruption Commission chose a "zero-tolerance" or "clean-hands" policy approach, which is a typical anti-corruption initiative. This initiative was considered appropriate and applicable in any economic sector (Quah, 2017). Critics to such an initiatives highlighted that it may encourage people to hide or cover up corruption more efficiently, making it more difficult to detect, hence the need of secret services to unearth covert criminal operations (Dupuy & Neset, 2018). While zero tolerance is merely a goal, ensuring that it is achieved necessitates taking into account the psychological and sociological elements in the environment that influence human actions (Tu et al., 2020). As an example, children raised in corrupt surroundings are more receptive of corruption, and few have ethical objections to bribery (Abun et al., 2020), this implied that strict policies are both a necessity, but also opposed. Organisations, industries or a government which seek to come up with effective fraud counter measures needed to come up with all round measures that focus on the employee, systems in the organisation and as well as collaboration with security intelligence apparatus. Developing measures focused on one aspect would rather create loopholes for more fraud crimes that would go unnoticed.

2.16 Insurance Intermediaries

The dispatch and distribution of insurance services and information has been a challenge in Zimbabwe, particularly micro insurance targeted at low-income earners across the country even to the most remote areas which lacked mobile phone network reception. The challenges were not only limited to distribution, but insurance fraud was on the rise in this particular market segment of the insurance industry (Muradzikwa 2021). However, the continuous modernisation of Zimbabwean societies, which was associated with technological advancement and the internet of things, insurance companies over years explored various means of distribution of insurance services and information. The explorations focused mainly on efficient distribution of micro insurance services and minimisation of micro insurance fraud. This prompted the formation of strategic partnership with other service providers operating particularly in those remote areas. This was against the backdrop that the Zimbabwean government had prioritised micro insurance, viewed as an important risk management mechanism for both individuals and business entities, but the primary focus of issuance of insurance services to low income earners was over emphasised. In Zimbabwe, insurance has been made available in a variety of forms; an assessment by the Insurance Association of Zimbabwe (IAZ) (2021), the method of distribution had limitations for it to stretch to low income earners. The employment of insurance brokers was and is the most common insurance distribution strategy and has provided that platform and means of micro insurance services to stretch to low income earners in Zimbabwe. In the domains of insurance solicitation, negotiation, and sale, intermediaries, often known as "brokers," or "agents," since year 1982 provided guidance, information, and other related important services to this market segment in Zimbabwe. Evidently, insurance intermediaries necessitated the penetration of micro insurance because parent insurance companies equipped the "brokers or "agents" with after sales services and other related services capabilities that complemented the insurance placement process. In that regard, intermediaries served a unique and multifaceted role in the insurance market. Their responsibilities included selling insurance products and services; they had in input determining insurance rates for low income earners, provided insurance service, and exhibited a keen understanding of insurance buyers' demands. The primary function of insurance intermediaries in the micro insurance services was to distribute insurance services and ancillary services to low-income earners who were previously excluded. Intermediaries brought a number of innovative aspects to the insurance sector that helped to expand insurance availability, with the government, non-governmental

organizations (NGOs), societies, and insurance corporations all benefited from intermediary activities to expand insurance distribution across the country. The how part of it was also recognised import? Insurance intermediaries introduced cutting-edge technology based marketing techniques to the insurance industry. The application of such technology was still at its infancy amongst micro insurers. Micro insurance companies hesitated to invest in such innovative cutting-edge marketing and distribution technology. The cutting-edge marketing and distribution technology deepened and broadened insurance markets by raising consumer awareness, it provided real time information of nearest micro insurance service providers, insurance policy rates, as well as a variety of insurance options available and how to obtain the insurance required. Customers and potential policyholders obtained any form of information from intermediaries' to initiate purchasing decisions. Due to internal training, they got from the principal insurance company, intermediaries responded to information requirement from policy and potential policyholders, responded to frequently asked questions, clarified customer needs as well as the many insurer policies and pricing alternatives available. When faced with a well-informed customer base with a variety of options, insurers offered plans that meet their clients' needs at a competitive price. Intermediaries also gathered and evaluated information on placements, premiums, and claims experience. The gathered data informed intermediary's knowledge of clients' needs, hence most intermediary were positioned to promote and assist the development of new and innovative insurance products, as well as to establish new markets where such insurance services did not exist. To complement efforts by insurance intermediaries and also avoid catastrophic losses, insurance companies positioned and guaranteed to provide insurance cover that was insurable and that insurance risks were properly spread. In that regard and with an objective to distribute insurance service across the board, insurance companies used intermediaries to help them with the difficult task of risk dispersion across their portfolio widespread distribution. Intermediaries worked with a variety of insurers and clients, and they frequently operated across a vast geographic area. They helped carriers spread risk throughout their portfolios based on factors such as industry, region, volume, insurance line, and other factors. This prevented overexposure of insurance companies to a specific region or type of risk, allowing valuable resources to be used for other objectives. By assisting insurers in lowering costs, broker services reduce the insurance costs of all undertakings in a country. Because insurance was recognised a necessary investment for all small scale enterprises and low income earners, a price reduction had a significant impact on the broader

uptake of insurance services by potential policyholder and boosting the market's overall competitive position. Insurance intermediaries played a pivotal role in the distribution of the micro insurance services. Individuals and groups of people operating village savings schemes that had lived in poverty and had created ways to deal with the risks that they faced throughout history were afforded an opportunity to a cost effective and reliable type of insurance.

According to McCord and Roth (2006) of the micro insurance centre for the United States Agency for International Development (USAID), the success of micro insurance was determined by a number of factors. Intermediaries designed demand-driven micro insurance solutions, solutions created to directly target the needs and capacitate low-income earners. Insurance companies in collaboration with intermediaries' further ensured reasonable cost effective premiums with sufficient coverage, be making sure that micro insurance products, as well as the mechanisms for delivering and servicing them, were efficiently managed. In response to the market's enormous development potential, new micro insurance distribution strategies were also developed all around the world. Evidence from a variety of pilot programs, as well as those that are already in full deployment is that the issue of intermediaries in Zimbabwe also included the intermediary's ability being able to deal with low-income earners on a regular basis. This, according to the Insurance and Pension Commission (2020) simplified premium payment, eliminated the need for a policyholder to make a special journey just to pay their premiums. The success of micro insurance distribution agents also depended on trust. The insurance intermediaries had their clients or customers' trust; potential policyholders also needed to trust the service providers as well. An observation by the Insurance and Pension Commission (2019) revealed that the opinions of the marginalised, low-income earners toward insurance were invariably negative at first. Trust of the intermediary by the policy holders and potential policy holders was therefore essential.

2.17 Role of Security Intelligence Organisation in Countering Insurance Fraud

The primary objective of the security intelligence department in Zimbabwe is to detect and thwart threats to national security and interest that emanates internally or externally by way of providing intelligence to policymakers and the President (President's Department, 2019). State organisations that gather, analyse, and disseminate information relating to risks to national security and interest are known as security intelligence or intelligence services and

sometimes referred to as secret services. Their roles are noted only limited to intelligence collection, but stretch to designing and implement counter measures though they have since inception of secret service preferred to remain secret and unknown. Military intelligence, internal security intelligence, police intelligence, foreign and internal intelligence, depending with the country are all tasked with the provision of intelligence to detect threats and coming up with counter measures. On a national and international level, intelligence comprises institutions responsible with insurgency, investigating terrorist financing and preventing money laundering (Hello & Peter, 2005). Security intelligence services by virtue and natures of their work are in a unique position to help identify emerging threat to national security while also assisting in the rejection of obsolete risks. Domestic or internal security intelligence agencies have a monitoring and analysis role, targeting a number of threats, including organised crime, insurgency groups and terrorist networks that often have international ties. While domestic or internal security intelligence agencies do not serve a law enforcement function, the information they generated has helped governments, policy makers and law enforcement agents in coming up with outer measures. A term referred to as operationalisation of intelligence in secret service (Mandez, 2019)

In Zimbabwe, the security intelligence organisation which is known as the Central Intelligence Organisation (CIO), but operates under the cover name of the President's Department (PD) is a secret service organisation that is responsible for the collection, analysis, exploitation of information and covert countermeasures in support of the President and other security organisations, namely Zimbabwe Republic Police (ZRP) and Zimbabwe National Army (ZNA). Further, the organisation has an advisory role on matters pertaining to national security and interest. Its advisory with authorisation from the Director General can be stretched to government department and regulatory authorities with special reference to issues of threats to human security, national interest and objectives. On establishment of the organisation in 1980, the objective was to insulate the President and policymakers from threats by eliminating or reducing uncertainty through foreknowledge (Clapper, 1995). Timely and accurate intelligence reduces the chance of intelligence failure and illuminates' decision by policymakers that enhances national security. Policymakers have diversified sources of information, but security intelligence was and is one of the most vital components when dealing with issues of national security and interests (Gates, 1994). The Central Intelligence Agency (1991) one of the leading intelligence agencies in the world has provided

a basic definition of intelligence as the “knowledge and foreknowledge of the world around us, the prelude to Presidential decision and action”.

The role of security intelligence organisations and agencies around the world has however, changed from state-centric, focused only on traditional threats namely subversion, insurgency, espionage, sabotage, and assassination (SIESTA) to non-traditional, human-centred threats such as economic threats, technological threats and human security, subversion, however, remains the mother of all threats (President’s Department, 2019). The President’s Department (2019) threat level assessment report confirmed that thirteen (13) major threats which faced Zimbabwe are in descending order organised crime, fraud, insurgency, geopolitical and geo-economic tensions, depletion of special resources, food insecurity, terrorism, religion, mass migration, bioengineered pandemics, nuclear warheads development, climate change and technological advancements. With the exclusion of climate change, the threat assessment report confirmed that the other twelve threats are linked to organised crime in one way or other and at some point financed with funds obtained through insurance fraud. The threat level assessment report categorically specified that micro insurance fraud is on the increase in Zimbabwe in the following insurance service providers, namely Old Mutual Life Assurance, First Mutual Life Assurance, Zimnat Life Assurance, Gesture Life Assurance, Econet Ecosure Life, Nyaradzo Group Life Assurance, Zimbabwe Bank Life Assurance, Fidelity life and Commercial Bank of Zimbabwe Life Insurance. Identified reasons for the increase in micro insurance fraud were that organised crime syndicates were taking advantage mainly of the low literacy level amongst most low-income earners in Zimbabwe and as well as poor countermeasures by the insurance companies. The insurance companies which were offering insurance services to low income earners irrespective of poor internal systems, hardly invested in artificial intelligence, an attempt to combat insurance fraud. The President’s Department Director-General, Moyo (2018), the Zimbabwe security intelligence organisation was mandated to intervene at all level once certain that national interest and security are threatened. Insurance fraud peddled by organised crimes syndicates was categorised as a threat to national security considering that it was distorting and disturbing economic development and financed insurgency and terrorism in Mozambique hence posed a regional threat as well. Further, insurance fraud in the micro insurance market was compromising national interest by compromising social security nest development for low-income earners who constitute seventy-five per cent of the Zimbabwean

population estimated to be fifteen million one hundred seventy-eight thousand nine hundred and seventy-nine (Zimbabwe National Statistics Agency, 2019).

Intelligence operations, on the other hand, though they require meticulous planning and highest level of secrecy, various organisations both public and private have since tapped into capabilities of security intelligence organisations to counter threat to their organisations. However, there is a distinction to be made between intelligence and security functions since they demand different management styles and different relationships with policymakers. Security intelligence that is effectively-managed was viewed as a key goal of human security and development, as well as a driver for economic progress (President's Department, Economic Intelligence Training Manual, 2018). In that regard, secret services are now recognised as a valuable source of lawful security by development agencies. Security agencies, such as the military, have strived to provide comprehensive protection against obvious and present risks, while the police in any nation are reactive and only act once a crime is committed; they are hampered by political sway and institutional inertia. However, security intelligence organisations had become the leading security apparatus that are proactive in nature and can be covertly deployed. Although arguments by other security forces such as the police and army that intelligence services are unable to provide complete security considering that by establishment, the number of officers in intelligence services are relatively few compared to the police and army, but the strength of secret services has lied in capabilities to discover emerging threats and operating in secrecy (Goodman, 2000).

2.17.1 Intelligence Cycle and Counter Insurance Fraud

One of the functions of a security intelligence organisation is to produce intelligence. Intelligence is different from information hence an intelligence cycle was a tool developed by intelligence organisations to produce intelligence by way of separating information from intelligence. Information is knowledge communicated about a particular fact or circumstance while intelligence is processed, accurate information presented to decision-makers (Sfetcu, 2019). Intelligence was created through a series of stages in a process known as the intelligence cycle, in which data and information were analysed to develop knowledge that is important in a country's defence (Sfetcu, 2019). Sfetcu (2019) ascertained that the intelligence cycle has four purposes, that is, ensure accuracy of information, timely dissemination of intelligence, avoid intelligence failures and enhance communication between officers and their commanders. The intelligence cycle, in this context, is a method

for transforming data and information into intelligence that was meant to benefit the enterprise or the country, a technique used to produce intelligence (Bean, 2018). The intelligence cycle varied from country to country Figure 2.4 below however depicts a basic eight continuous stages of the intelligence cycle.



Figure 2.4: Intelligence cycle

(Source: President’s Department Training Manual, 2018)

The President and the Director-General of the President's Department determine the intelligence requirements in cooperation with other security agencies such as the Zimbabwe National Army (ZNA), the Zimbabwe Republic Police (ZRP), and the Zimbabwe Prisons and Correctional Services (ZPCS). Security requirements are set at the beginning of the year and are continuously upgraded throughout the year and they are threat informed. It is at this stage, that the President can issue a directive to consider organised crime and insurance fraud as a threat to national security and in that it becomes a target. In response to the intelligence requirement (IR), security intelligence organisations, through units, will covertly and overtly collect information with regards to the security targets. Collection appears to be a simple

intelligence activity, and its necessity is not questioned. Information is gathered from both overt and covert sources. Intelligence agencies collect information about targets, places, events, and activities that the Zimbabwean government requires to counter all threats to national security using a variety of methods. Open-source intelligence (OSINT), signals intelligence (SIGINT), images intelligence (IMINT), and human intelligence (HUMINT) as information collection tradecraft are all available to the organisation (Basic Intelligence Course Training Manual, 2019). The collection function of an intelligence and security organisation depending with the directive have targeted individuals, groups and even organisations involved in insurance fraud. The collection of intelligence does not only focus on collecting historical data, it also focused on profiling the individuals and accounting for their day-to-day activities (Brantly, 2016). Intelligence analysts link data from open-source intelligence (OSINT), signals intelligence (SIGINT), images intelligence (IMINT), and human intelligence (HUMINT) to generate operational intelligence during the information analysis stage of the collection process.

Intelligence processing entails gathering and interpreting available data. Information must then be interpreted after it has been processed. This means it is compared to all other available data in order to answer four basic questions known as the 5W and 1H (Who, Where, What, When, Why and How). The interpretation phase of the intelligence cycle serves as a point of departure in profiling members of organised crime syndicates (Hart, 2011). Dissemination is the communication of intelligence to the intelligence consumers (President's Department, 2016). The President's Department (2016) has used various forms of intelligence dissemination such as written or verbal briefs and routine intelligence summaries. The effectiveness of intelligence lied in the accuracy, reliability and timely dissemination, with a clear distinction between intelligence fact and interpretative comment or assessment (Sfetcu, 2019).

2.17.2 Taking action:

Taking action is the action phase of the intelligence cycle. Countermeasures usually are put in place in the form of intelligence operations, in some cases referred to as covert and or clandestine operations. Covert action as a function of a security intelligence organisation can counter organised insurance fraud through the following:

- **Countering organised crime.** The focus of security intelligence in countering organised insurance is primarily premised on accurately identifying individuals within

the syndicate, identifying their leadership hierarchy and profiling the activities of the syndicate. Furthermore, an understanding of their influence on the political systems and tradecraft capabilities may include software and hardware, cover and concealment (INTERPOL, 2018). The security intelligence organisation should further expand its covert operations by also thwarting other crimes financed by organised crime syndicates, particular focus should be on counter human trafficking, drug and weapons trafficking and insurgency. A study of the tactics by insurgency groups entailed recruiting and transferring people into exploitation situations through violence, deception, or compulsion, and forcing them to labour against their will (Counter insurgency training manual, 2017).

- **Counterterrorism:** As an important component of human security, the security intelligence organisation should also focus on identifying and countering threats to its citizens and facilities that could be a target for terrorist attacks. This activity also includes providing a warning to other countries of terrorist activities within their territory. Terrorist groups strive to finance their activities from money easily obtained from insurance fraud (Ministry of State Security, Zimbabwe, 2020).
- **Counternarcotic.** Security intelligence organisation should also gather and provide intelligence to drug enforcement authorities to prevent drug shipments. A 2017 intelligence lead investigation unearthed that prominent drug cartels in Zimbabwe have financed the purchase of drug processing equipment with money obtained from the Air Zimbabwe aircraft insurance fraud (President's Department, 2017).
- **Counter proliferation:** Intelligence and security services counter the illegal development and transportation of weapons in a way that violates international law. Organised crime syndicates are always seeking funds to purchase, bribe government officials and transports weapons to other countries. The weapons have historically armed insurgency groups in Mozambique, with a possibility of regional destabilisation (Ministry of State Security, Zimbabwe 2020).

Reassessment: This is the monitoring and evaluation process of intelligence operations. The purpose is to determine, the intelligence failures and success of an intelligence operation.

2.18 The Missions of Intelligence

Intelligence function is not complete without the complementation of the security intelligence missions. It is the responsibility of the Zimbabwean President to select necessary and

appropriate missions for the security intelligence organisation including other security forces with a primary objective to advance national security and national interest (President's Department, 2017). According to the Interpol (2019) overview report on serious and organised crime in Africa, intelligence missions are important considering that they allow for joint operations or interstate security intelligence operations in countering activities of organised crime syndicates. Depending on threat level assessment, traditional missions of security intelligence missions vary from support to diplomacy and policymakers. This entails providing real-time intelligence on global threats with the likelihood to affect the security and interests of individual countries. Such intelligence gives policymakers, security intelligence analysis and intelligence operations personnel competitive advantage in designing appropriate countermeasures.

The collection of economic intelligence is becoming a leading mission for intelligence organisations with a focus on human security. Amongst the plethora of economic targets, insurance is a major target considering its impact on economic development. The primary goal of this mission is to give intelligence on areas that potentially have an impact on national interests, such as foreign country economies, global economic trends, and information to aid trade talks. Furthermore, an assessment of how organised crime syndicates' activities relating to terrorism, fraud, drug trafficking and weapons proliferation affect national and international economics (Ministry of Home Affairs, 2017). Intelligence agencies also respond to requests for intelligence information about foreign persons or businesses from a range of regulatory bodies, such as foreign companies applying for a license to operate in Zimbabwe or foreign individuals seeking a visa to enter Zimbabwe. Such a mission if managed and monitored in accordance becomes the first line of defence in identifying and filtering criminal elements amongst individuals and companies hence they can be deterred to operate in other countries.

2.19 Tradecraft

Within the intelligence community, tradecraft refers to the capabilities, strategies, methods, and technology employed in modern espionage and, more broadly, as part of the intelligence assessment effort to detect and neutralize threats to national security and interest emerging from within or outside the country (Robert Gabriel Mugabe School of Intelligence Training Manual, 2020). Tradecraft, according to Danigelis (2012), are skills deployed by intelligence personnel to build ingenious disguises, perform surveillance, use concealments, obtain secret

information, and exchange secure messages with other agents. The skills are obtained through rigorous training in what is called the basic and advanced intelligence course. Such skills are only trained to intelligence officer and are not found in any other organisations worse the private sector. An analysis of counter insurance fraud operations conducted in Zimbabwe have revealed that intelligence personnel a knack for coming up with creative ways to covertly infiltrate and communicate with organised crime syndicates (Classified Intelligence Briefs on Insurance Fraud, 2020). This provided them with covert access to organised crime syndicates that prey on the insurance business. The main goal was to detect and counter threats posed by these organised crime syndicates targeting insurance companies offering services to low income earners. Agent acquisition and handling, or the administration of espionage agents, also known as informants, sources and contacts, major are examples of tradecraft tactics. Clandestine surveillance through the use of cameras, audio equipment for listening to conversations, and undercover operations are all examples of tradecraft capabilities has been effectively deployed, utilised to supplement existing intelligence gathering capabilities in the insurance sector to expose criminal activity.

2.20 Agent Acquisition and Handling

An agent is a person who is aware that he is involved, engaged in clandestine activities and accepts some degree of control from an intelligence officer. Agent acquisition is the process of identifying and recruiting a potential agent while agent control is the influence used by the intelligence officer to direct the agent to accept some instructions, direction and discipline of a clandestine operation. It is imperative at this stage to note that, depending with the intelligence organisation, an agent is also called a source by virtue of being a source of information of intelligence value. The Zimbabwe intelligence community (2018) referred a source as a person under the regular direction and control of a source runner (intelligence officer) who gathers information secretly and is consistent in access and reliability. Generally, there are two types of sources, that is, a clean source and a turned source. A clean source is person chosen for personal qualities and characteristics, who is recruited and then seeks access to a target while a turned source is a person already in alongside a target who is recruited to provide information with regards to the target organisation or individuals. Intelligence organisations act on accurate information and they take their time in designing strategies to gather the most accurate information. It is against this backdrop, security intelligence organised invest human and financial capital in identifying, recruiting and

nurturing well-placed sources and contacts. It is this type of capabilities, tradecraft which security intelligence organisation can deploy to gather accurate information about activities of individual and groups involved in organised insurance fraud. Constanza (2014) contended that there has been a serious need to continuously identify and recruits' fresh sources of raw intelligence in generating strategic intelligence that meets the requirements of policy makers. To satisfy new sets of need in growing areas of interest to intelligence analysts, new sources are constantly required. It is against this background that there is a need to recruit new sources that can either infiltrate organised insurance fraud groups; or, secondly, individuals within these groups to provide real-time intelligence with regards to operations of the group. Agent acquisition is an expensive, delicate and perilous process; it requires serious attention to detail, good analytical skills and highest level of secrecy, failure which can compromise the whole operation by security intelligence personnel to contain organised crime syndicates. An operation to identify individuals and groups involved in organised insurance fraud is a long term, expensive and risky intelligence operations. It requires a massive investment in human intelligence sources, specific electronic surveillance gadgets and weaponry. Informants or human sources are therefore not haphazardly recruited, but rather a laid procedure that ensures that a right source with capabilities to operate in secrecy and with the required access is recruited (Moyo, 2019). This agent recruitment process is made of seven continuous steps, namely establishing the requirement, finding potential agent, assessing suitability, approaching and recruiting, running the agent, recording operations and finally termination and settlement.

2.20.1 Establish the requirement

An intelligence requirement (IR) relates to any form of intelligence (information) required by decision makers and policy makers. In that regard, intelligence requirements are laid down by management and these requirements spells targets for monitoring which may include organised crime syndicates in organised insurance fraud. The FBI Office of Intelligence (2004) explains that:

... the same phenomenon applies to the operational world of criminal intelligence. To adequately assess the threats from a terrorist group or criminal enterprise, information is needed for a comprehensive analysis. Oftentimes during the course of the analytic process, critical information is missing that prevents a complete and accurate assessment of the issue. This is a gap, an unanswered question related to a criminal or terrorist threat. An intelligence

requirement is identified and information needs to aid in answering questions related to criminal or terrorist threats...

2.20.2 Finding a potential source

Finding the potential source comprises two components, namely target analysis and talent spotting. Target analysis is the systematic analytics of the identified target so as to establish modus operandi, objectives and motives. This entails profiling which informs behaviour prediction analysis. The profiling will focus on bio data, professional background, educations, vices, social life and political inclination. Such information can be obtained from already collected intelligence within the organisation, open sources and from other sister security organisation and through surveillance. target analysis analyses the suitability of an individuals within a target organisation to be engaged in clandestine operations, also known as talent spotting. Talent spotting henceforth is the selections of a potential suitable candidate for recruitment within the target organisation. Talent sporting starts from general to specific after profiling of the targets to determine their suitability for the operation.

2.20.3 Assessing suitability

Assessing the suitability of the candidate involves security vetting, candidate investigation, candidate assessment and candidate development. The identified candidates will have to go through the selection vetting and assessment, which is meant to fully identify the candidate in terms of motivation to provide information, personal characteristics, family background and circumstances, capability to live under cover and most importantly access to the required information. The information gathered will eventually inform the decision maker to either recruit the candidate or not. Once the assessment and vetting has been done, the following stage is candidate investigation. Candidate investigation is purely meant to establish gains and risk involved in the operation. Candidate investigation will focus on commitment, loyalty, vices, reputation and public responsibility of the candidate in relation to the operations he is required to do.

2.20.4 The approach and recruitment

Recruitment of the source is a delicate process which should be approached with care. Recruitment is the process of persuading and convincing a potential source to accept to be involved in a clandestine operation.

2.22.5 Running the source

Running the source involves the tradecraft of source running. Running the source in this regard comprise meetings, briefings and debriefings. This is the secret information sharing between the source and the intelligence officer. It is of great importance that the source runner establishes a secure means of communicating with the source. This can be achieved by, first, establishing a good cover story; and secondly, agreeing on the methods of briefing and debriefing, that is, either face to face or using dead and live letter boxes. Further, the administration of the whole process that is secret payment of the source for services offered.

2.20.6 Recording the operation

Recording the operation in source running should be done in two ways. That is through the maintenance of a source file and through intelligence reports. The briefings and debriefings with the source should be recorded on the running diary section of the source files. This should also include reports and documents provided by the source should be filed on the report section. Eventually, the intelligence officer produces report, come up with a threat assessment and eventually recommend course of action.

2.20.7 Termination and resettlement

One the operation has achieved its objectives and complete, the source should be terminated. Source termination is a process whereby the services of a source are coming to an end and the source is made aware of the fact and the conditions for ending such services. The termination of a source operation is delicate considering that, if not done procedurally and in agreement, might lead to the compromise of the whole operation. In that regard, the officer responsible should make sure that promises made during recruitment are fulfilled; prepare briefing for the termination which should include the need to main secrecy. However, sources who would have been involved in dangerous operations can be settled by being relocated to other countries offered new identity particulars and possibly a job.

2.21 Profiling

Target profiling is a method of determining a person's mental, emotional, and personality qualities by extrapolating data from known traits, tendencies, observed characteristics, and behaviours. Targeting profiling in intelligence is meant to predict behaviour based on a series of historical behaviours. In security intelligence, target profiling is based on a combination of past and present behaviours. Every human encounter involves profiling. During daily interactions, people have a tendency to automatically judge the behaviours of others. It is a

natural social process to be curious about another person's personality, character, and even intentions. Profiling is a type of retro classification, often known as reverse engineering, which is a classification method that works backwards. As a result, target profiling is a science in which basic research concepts are used to obtain basic facts on a target. However, the most crucial aspect of target profiling is to obtain one hundred per cent accurate data, which is possible if the data is acquired surreptitiously. According to Douglas and Burgess (1986), profiling usually entails a thorough investigation of previous criminal act committed by a group or individuals, a thorough investigation of the crime scene's circumstances, a thorough investigation of the victim, and a thorough investigation of preliminary police reports. Additional steps include the creation of a profile comprising critical offender characteristics, as well as investigation ideas based on the profile's design.

Criminal profiling is very beneficial in cases of fraud, organised crime, hostage negotiations, identifying threatening letter writers, rapists, arsonists, and sexual killers. According to the President's Department Training Manual on Basic Intelligence (2015), profiling in intelligence helps to detect and or predict behaviours of already known criminals. It is therefore important to always have personal information of these already known criminals and as well as keep them under watch to gather further information. Personal information is any data that can be used to identify and distinguish one person from another. A person's biographical data, which includes their name, residence, gender, marital status, and date of birth, is the most basic of this information. It is critical to understand what a biodata file is, what information is frequently sought, and why the information is relevant to the person or organization making the request.

When profiling an individual, knowing and having rapid access to more than the target's basic information is critical. An officer can also enter and track an individual's various phone numbers and addresses (street, email, and uniform resource locator), as well as data about the individual's ethnicity, visas and permits, citizenship and passports, languages, relationships, religious preference, emergency contacts, and work experience. Through biodata profiling, the organisation or anyone, even without seeing the person would want to know the target in terms of name, identity passport number, date of birth, contact information, residential address, genotype, race and place of origin to mention a few. Button, Pakes and Blackburn (2011) averred that offender profiling, in which essential features of offenders are discovered with the goal of improving fraud prevention and detection, has sparked a lot of

attention. There have been several attempts to profile fraudsters, but most of them have tended to focus on internal occupational fraud against businesses, while some have also included external fraudsters. However, intelligence organisations have commended target profiling since it has assisted in categorising organised crime syndicates according to crime specialisation.

2.22 Surveillance and Counter Organised Crime

Surveillance is the act of keeping a person, group of people, area, security installation, and building, vehicle under secret observation for the purpose of collecting intelligence and to some extent restrict. The President's Department Training Manual on Surveillance (2018) explained that surveillance has various purposes that can be applied in countering insurance fraud by organised crime syndicates. Surveillance is precisely meant to obtain evidence of a crime or unauthorised activity, obtain detailed information about the organised crime syndicates activities, and develop leads from information received from other sources. Surveillance has also been a secret mechanism to know the whereabouts of an individual at all times, gather information that will be used for further investigation or interview of suspects and to locate and account for individuals in an organised crime group. The Association of Certified Fraud Examiner (2018) concurs that surveillance, as a security intelligence tradecraft technique, can be applied in countering insurance fraud. The association defined surveillance as the planned observation of people, places, or objects (The Association of Certified Fraud Examiner, 2018). People are usually the focus of surveillance. The observation of places and other related items is frequently secondary to the primary goal of acquiring information on specific people. Surveillance is a method that insurance investigators have deployed for a number of purposes. According to the Association of Certified Fraud Examiners (2018) insurance companies have deployed surveillance to monitor and determine the degree of a claimant's stated injuries, locate allegedly stolen or damaged property, locate witnesses, determine claimant identification if previously unknown, and locate a health care provider to verify treatment are some of the reasons for utilizing surveillance. Surveillance has also been deployed to track down people's homes, businesses, and other locations of interest, and places where criminal activity is taking place. Further, on individual profiling, surveillance has proved to be effective on providing crucial evidence about the extent and character of a person's activity. In that regard, intelligence over a period of time meticulously documented surveillance operations hence building a profile. Tape

recordings, detailed notes and logs, audio and video recordings sometimes with special lenses and light sources are all part of surveillance techniques. To put it another way, surveillance is a nebulous approach with both positive and negative implications. Surveillance is sometimes conducted undercover. Each surveillance system has its own set of uses. One or a mixture of these methods may be employed, depending on the information needed. Surveillance as a tool for discreet investigations falls into four categories

2.22.1 Electronic surveillance

Electronic surveillance is the use of electronic devices such as close circuit televisions (CCTV), lawful wiretapping, cameras, digital video equipment, and other electronic, digital, and audio-visual techniques to covertly monitor and collect data from targeted houses, businesses, or individuals. The information collected while the targeted audience is unaware. Electronic and technical surveillance has changed immensely to support the observation of individuals, homes, offices, and even entire cities, as electronic gadgets have become smaller, more powerful, and more linked. Listening devices, also known as 'bugs' or 'wires', lawful interception, wiretapping or telephone tapping, mobile phone data, including location information can constantly be collected and stored. These gadgets are becoming more sophisticated and powerful, and new approaches like lamphone are being developed. These can be deployed for audio visual monitoring of organised crime syndicates. Intelligence operatives with such capabilities have monitored the movement, conversation, bank accounts, contact list on telephones and email of these syndicates, with an objective to unearth future plans. Depending with the situation or threats, electronic surveillance can be deployed targeting specific individuals or groups in a specific crime (Moyo, 2020). When an insurer suspects that claimants have overstated or increased their claims or are engaging with organised criminal syndicates, insurers can properly monitor a policyholder's actions and even request the service of security intelligence to assist. Insurance companies are often allowed to monitor an individual in public places where the person does not have a "reasonable expectation of privacy".

2.22.2 Static surveillance

Static surveillance, often known as "stakeout", is whereby officers quietly watch persons and sites from afar. The one- and two-person surveillance methods are examples of variations. The two-person strategy, according to Heibutzki (2018), permits officers to exchange positions on a regular basis, minimising the odds of a suspect being noticed.

2.22.3 Mobile surveillance

Mobile surveillance comprises foot and vehicle surveillance. Both vehicular and foot surveillance provides unique problems, yet both have a same goal, that is, to remain undetected by hiding in plain sight. Any surveillance operation's success is greatly dependent on preparation, and a good surveillance operative should be prepared to switch from mobile automobile to foot monitoring at any time.

2.22.4 Tracking

The act of determining where the target has gone and where the target has been is known as tracking. Time frames differ. Investigators may practically follow a target around invisibly at times. Investigators may also employ various tracking technology. GPS tracking and location applications are examples of these technologies.

2.23 Undercover Operations

Undercover operations are a type of surveillance in which the case intelligence officer plays a more active part in uncovering illicit activity. Investigating organised crime, narcotics crime, extremist groups, and vice activities requires covert undercover operations that conceals the intentions and identity of the case intelligence officer. Most cases of insurance fraud have gone either undetected, if detected lack of sufficient evidence to secure conviction (ZRP, 2016). It is against this background that detecting and acquiring evidence or proof of covert illicit deals that do not immediately involve complaint victims, undercover operations are necessary. Insurance fraud and public official bribery are two examples of illegal activity that can only be combated by active and effective covert undercover operations. For example, intelligence personnel might start infiltrating the group by taking up the same hobbies as the suspects, becoming friends with suspects and eventually opening up on private issues. The intelligence officer should however, establish a credible cover story that explains his presence in the neighbourhood, associations with certain individuals in order to win acceptance and trust inside the gang. Covert operations are thus, a low-cost, low-risk technique to burst activities of organised crime syndicates. According to a 2018 study by University of Chicago political scientist Carson (2018), covert operations may have the benefit of preventing conflicts from escalating into full-fledged geopolitical tension, because combating organised crime syndicates may require intelligence officers to cross national borders and operate in other countries as undeclared officers. Secret, uncoverintelligence operations have helped

states to limit the escalation dynamics and protect leaders from domestic pressures while also allowing them to convey their intentions and achieve their goals.

Intelligence officers and other law enforcement agents with an intention to cross national boundaries, penetrate criminal organisation to obtain evidence, undercover operations trade craft maybe be deployed. However, well-managed and adequately trained personnel should conduct undercover operations. The goals of undercover intelligence operations is to ascertain the type and scope of criminal activity identify those engaged, and gather evidence that will allow criminals to be charged and prosecuted. When it comes to planning and executing undercover operations, the safety of undercover operatives is paramount. The hazards presented to agents, victims, and their families should be considered in the planning and execution of the operations, as with any investigative procedures (UNODC Operational Training Manual, 2008).

2.24 Conclusion

Chapter two (2) provides an insight of the threat of insurance fraud and framework of how security intelligence can counter insurance fraud in the low income sector. A concern with regards to the impact of organised crime syndicates which are targeting micro insurance service providers has since gravitated to become a human and national security threat. The literature in this chapter demonstrated that there is need for integrated intervention measures. Insurance companies and insurance regulatory authority in Zimbabwe together with the state security intelligence apparatus should develop strategies both internal and external to the insurance companies that equips with detection, investigation and deterrence of insurance fraud. However, in order to come up with such strategies this chapter categorically explained that it is important to have an understanding of what is insurance in general and micro insurance in particular. Further to this, a dissection of the importance of micro insurance in the low income sector of Zimbabwe and how insurance fraud has over yeas compromised this position.

The following chapter details theoretical reviews on the causes of insurance fraud. Evidence from previous research will guide in the formulation of micro insurance fraud counter measures in Zimbabwe. The theoretical review dissects and inform on conclusion with regards to causes of insurance fraud and also a synopsis of possible counter measures that can be adopted at company and industry level.

CHAPTER THREE

THEORETICAL REVIEW

3.1 Introduction

Chapter three of this study examines research, empirical findings, evidence and approaches underpinning the causes of insurance fraud. The prime objective of the theoretical review was to understand the causes of insurance fraud, its effects which is the departing point in coming up with counter measures that can be deployed by individual insurance companies and also an industry approach in countering insurance fraud. Further, a synopsis on how the counter measures can be fused with security intelligence considering the surreptitious nature of insurance fraud. A synthesis of research from scholars and professionals in insurance industry, government publications, academic journal articles, and published and unpublished theses were used to unpack underlining issues in insurance fraud. Weisbur (1995) previous research on insurance fraud in the low income sector generally focused on fraud perpetrated by corporates and individuals, but there is a need to stretch research to insurance fraud in the low income sectors perpetrated by organised crime syndicates, with an objective to unpack the causes, reasons why organised crime syndicates are targeting the low income market segment and also the threat posed such criminal activities to individuals, corporates and the government.

Insurance fraud in the low income sector is increasingly becoming a global threat. Insurance companies and organisations in general, are seized with a task to come up with countermeasures both at the company level and at the industry level. According to the Association for British Insurers (2016), insurance companies in the future will deploy their artificial intelligence and commercial strategies to possibly minimise insurance. However, this will not stop insurance syndicate fraud at company level and within the industry, unless all insurance companies have partnered and pulled in the same direction. More so, a well-established fraud control task force both at company and industry level working in liaison with state security intelligence apparatus will go a long way in countering organised insurance fraud. Research done so far in economically advanced economies has recommended the need for a prior understanding of causes of insurance fraud before designing counter measures. It is against this backdrop that the theoretical review of this study sought to identify the causes of insurance fraud both at the company and industry levels.

3.2 Fraud Triangle

An understanding of why individuals commit fraud is emphasised in the fraud triangle which was developed from preliminary research done by Cressey in 1950. Further development by Cressey (1971) identified three elements that have compelled individual to engage in the criminal act of fraud. The three elements comprise a non-shareable financial problem, opportunity and rationalisation or existence of an opportunity. Figure 3.1 below, diagrammatically depicts and summarises the three elements. The first element, pressure which is on the top of the fraud triangle triggers an individual to commit a crime. However, the pressure or motive to commit a fraudulent act triggers the desire, but does not work in isolation; it is complemented by the other two elements at the bottom fraud triangle, namely perceived opportunity and rationalisation (Cressey, 1971).

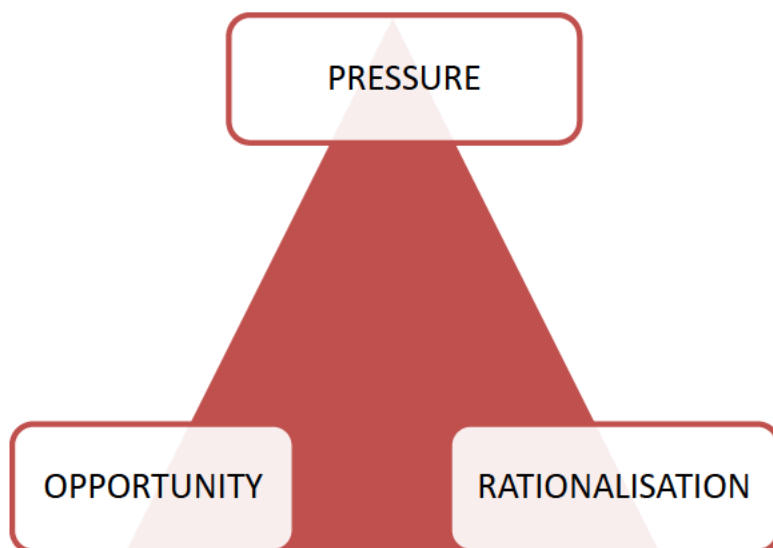


Figure 3.1: Fraud triangle

(Source: Cressey, 1971)

3.2.1 Pressure

Pressure also known as an incentive is the trigger or relates to the motivation that pushes an individual to commit fraud. An individual who engages in fraud first experiences some type of pressure to commit fraud. The word perceived is important, the pressure does not have to be real, and the individual should first believe and be pressurised to commit fraud (Albrecht, 2006). Perceived pressure emanates from various circumstances, mostly, from non-shareable financial problems. This varies from person to person and situation to situation. Greed, living

beyond one's means, excessive expenses or personal debt, family financial issues, health, drug addiction, and gambling are all examples of perceived pressure (Consumer Council of Zimbabwe, 2017). Financial incapacitation is however the universal driver or pressure of all forms of insurance fraud. Sources of pressure emanate from either internal to the individual or external to the individual (Abdullahi, 2015).

Some studies by Vona (2008) suggested that personal internal pressure combined with external to the individual and organisational are both proxies that compel an individual to engage in criminal conduct. Lister (2007) complemented the fraud triangle, and envisioned pressure as “the source of heat for the fire”, but the pressure alone does not guarantee that the individual will engage in criminal conduct. Murdock (2008) categorised pressure into four categories, namely social, political, financial and other non-financial pressures. Non-financial pressure is directly derived from poor financial management skills which subsequently lead to bankruptcy, addictive habits such as gambling and drug addiction. Social and political pressure could be due to the attempt to maintain one's status as well as managing general public perceptions in terms of financial status or reputation, hence compelling an individual to engage in criminal activities to earn extra money to maintain the perceived life style. Subramanian (2008) defined pressure as the key driver that motivates or drives an employee, policy holder or a group of people to commit fraud, the drivers may vary from greed, reputation or personal financial pressure. Vona (2008) concurred and averred that the motive to engage in criminal conduct such as occupational fraud often emanates from the individual but is complemented by corporate pressures. The motivation to commit fraud, on the other hand, can be triggered by pressure, then self-justification and an opportunity to commit fraud without being compromised, described as a state of safety. Muhammed (2014) transgression of obligations, individual issues, corporate inversion, position accomplishment, and employee relationships were recognised as basic triggers or pressures for one to commit fraud.

Recent literature suggested that the economic meltdown in Zimbabwe, which is associated with very low salaries and economic hardships has been a major contributor of organised crime syndicates fraud related crimes and occupational fraud (Zimbabwe Republic Police, 2018). Gambling and drug addictions, on the other hand, are the second group of factors that drive people to commit fraud. The increased incidence of fraudulent activity amongst employees in Zimbabwe, in conjunction with organised criminal syndicates, according to KPMG (2020), was primarily driven by financial incapacitation as a result of the country's

low economic development. The Reserve Bank of Zimbabwe's Financial Intelligence Units (2019), referring particularly to the insurance industry in Zimbabwe, reports that poor working conditions and unfair labour relations practices have resulted in workplace dissatisfaction. In this case, employees are not hesitant to commit acts of fraud in retaliation for the unfair treatment. Research within the insurance industry by the Insurance and Pension Commission (2018) identified unfair labour practices as the most common source of dissatisfaction amongst employees. Examples of unfair treatment included not being promoted on time, unfair remuneration, employee layoffs, unfair labour practices and or lack of appreciation. In micro insurance service providers resultantly led to high levels of disgruntlement amongst employees, lack of respect, no commitment and occupational fraud.

3.2.2 Perceived Opportunity

Existence of an opportunity is also a contributing factor. Perceived opportunity is the second element that triggers criminal conduct. Ineffective internal systems such as lack of artificial intelligence and poor internal control systems at company level combined with non-deterrence measures by the government and industry through proper legislation and policies create an opportunity for individuals to commit fraud. The employees, usually in connivance with organised crime syndicates exploit such weakness within insurance companies. In accounting, these internal control weaknesses are, according to KPMG (2013), the major factors attributing to insurance fraud. This concept proposed that an individual or a group of people will take advantage of loopholes, poor security measures and circumstances available to commit an illegal act (Kelly & Hartley, 2010). However, the opportunity can either be real or perceived. The belief and thinking by an individual or a group of people that an opportunity exists is sufficient enough to influence engagement in a criminal act. The individual or group involved also calculates and ascertains the risk of being compromised. Security is paramount. The existence of high chances of compromise could lead the individual or the syndicate to abandon their intention, but once the risk is low, chances are high that the illegal act would take place (Cresse, 1953). Furthermore, other factors related to perceived opportunity may include employees being aware that there are no internal security measures and constant checking of employees for violating organisational policies and procedures (Sausser, 2007). Andrew (2012) the ability of an employee to exploit internal weaknesses is also an opportunity that necessitates criminal conduct.

Hooper (2010) financial fraud occurs when an opportunity arises irrespective of the existence of pressure. The opportunity to commit fraud has two aspects, namely vulnerability and working conditions. Furthermore, Turner (2005) argued that motive alone is not sufficient to pressure one to commit fraud; an opportunity should also be available. Vance (1983) ineffective monitoring enhances the opportunity and individuals within an insurance company or externals to the company may take advantage of it. Poor organisational structure, ineffective controls combined with lack of supervision or inadequate segregation of duties may provide opportunities for different types of criminal acts including fraud (Udoayang, 2012). According to Singleton (2006), long-term saving employees are highly likely to engage in occupational fraud in an organisation considering that they are aware of the organisation's strengths, weaknesses, opportunities and threats to all forms of criminal behaviours, such employees successfully commit any form of occupational fraud without detection. However, it is generally assumed that suspected criminals and employees with a criminal record within an organisation are sensitive to the risk associated with fraud (Simpson & Koper, 1992) but continue to commit fraud because of various motives and the existence of an opportunity. Increased possibilities of compromise reduce fraud opportunities. Detection, particularly in the insurance industry, can be achieved through various such as the use of artificial intelligence and effective internal systems (Sarre & Fiedler, 1999).

3.2.3 Rationalisation

The rationalisation concept suggests that individuals convince themselves and formulate a morally acceptable reason before engaging in criminal behaviours such as fraud. Rationalisation is perceived justification that an unethical act such as fraud within an organisation is different from a criminal act (Abdullahi, 2015). If perpetrators of fraud cannot justify the criminal conduct, they are unlikely to commit the act. Organised crime syndicates, terrorist groups and insurgency groups all have justification for committing criminal acts. Justification depending on the motive and objective may vary from financial greed, and political to religious justification. Rationalisation among fraud perpetrators is unidentifiable considering that it is difficult to read through someone's mind (Cressey, 1953). Organised crime syndicates involved in criminal activities have a shared understanding and objective that allows them to justify and engage in criminal activities (Hooper, 2010). However, rationalisation emanates from an individual or group's lack of integrity or moral reasoning as justification for fraudulent behaviour (Rae, 2008). Other fraudsters, on the other hand,

recognise that their actions are wrong, but they are persuaded to continue with their criminal activities, primarily by group leaders in organised crime syndicates (Willott, Griffin & Torrance, 2001).

The propensity to commit fraud depends on people's ethical values, beliefs and norms. Personal circumstances also being a contributing factor. An individual's character and other external factors such as job insecurity, redundancy, and work environment shape a person's behaviour towards criminal activities (CIA, 2019). Consumers in the insurance sector defend their unlawful behaviour by pointing to the fact that they have been paying insurance premiums for years without receiving benefits. They engage in such behaviours as a means of recouping (Dean, 2004; Tennyson, 1997; CAIF, 2015). The cognitive dissonance psychological theory characterises reasoning as a criminal act in which people are required to create claims in order to engage in behaviours they would otherwise avoid (Kunda, 1990; Ramamoorti, 2008). Contrary cognitions are a form of cognitive dissonance that pushes people to adjust their thoughts in order to align them with their behaviours and avoid feelings of illegality and guilty (Kunda, 1990). Wilson (2004) defined "opportunity" as the ability to circumvent fraud measures, "pressure" as the impetus to perpetrate, and "rationalisation" as the moral and ethical justification for the conduct. Pressure, chance, and rationalisation are all intertwined, and the strength of each influences the others. Malgwi (2006) stated that an individual's ability to rationalise fraudulent behaviour creates a link between the three factors of opportunity.

3.2 Shortcomings of the Fraud Triangle

The fraud triangle had flaws since it was based on the assumption of an equal triangle with equally weighted variables on all three sides. In the literature, the fraud triangle has been modernised to a fraud diamond (Wolfe & Hermanson, 2004), or a fraud pentagon (Marks, 2009). Hermanson (2004) added a fourth aspect to the fraud triangle, that is, capability. Capability arises from or is aided by an employee's position in the organisation, as well as intellectual and cognitive attributes and abilities, allowing employees and potential criminals to perceive and exploit a fraud opportunity. Evidently, organised crime syndicates are usually comprised of people with different capabilities and educational background all that useful in their criminal endeavours. An employee's position inside an organisation gives them the power and access to create or exploit a fraud opportunity that anyone external to the organisation cannot. Wolfe (2004) suggested that fraudsters possess the necessary traits and

abilities, once they realise an opportunity to commit fraud they take advantage of it. Those traits include one's mandates within a company, ingenuity in using internal accounting systems to the greatest advantage and understanding how the organisation system works, ego and confidence that fraudulent behaviour will not be detected, and the ability to effectively deal with stress caused by the risk of being caught and managing the fraud over a long period of time (Hermanson, 2005). According to Marks (2009), an employee's competence and arrogance play a significant role in criminal actions. An employee's competency sets the conditions for fraud to occur, while 'arrogance' is the fifth factor in the fraud creation process. A perpetrator's attitude of superiority, entitlement, or avarice compels the individual to believe that business policies and procedures do not apply to them personally. The opportunity, on the other hand, opens the door for fraud, and incentives and reasoning can entice someone to do it. According to the fraud diamond hypothesis, an employee must be able to perceive and capitalise on opportunities. While a variety of factors may influence an individual's decision to commit fraud, the fraud diamond theory debate can benefit the fraud detection and prevention disciplines. The fraud diamond idea can be used in the intelligence and security matrix to design countermeasure that are informed by human behaviour (CIA, 2018).

3.3 Adam's Equity Theory

According to Adams' equity theory, a fair balance between an employee's "inputs" (hard labour, skill level, acceptance and excitement) and their "outputs" (productivity) should be accomplished (productivity, efficiency, salary, benefits, intangibles such as recognition, and more). Employees who achieve this fair balance, according to Adams' equity theory, contribute to the development of a strong and productive relationship, resulting in satisfied and motivated employees. Adams' equity theory, like many other famous motivation theories such as Maslow's hierarchy of needs and Herzberg's two-factor theory recognised a variety of nuanced and different factors that influenced an employee's perception of their work and employer. Employees get demotivated in their jobs and companies, according to the notion, if they consider their inputs higher than the outcomes they obtain. In that regard, employees may react in a variety of ways, including dishonesty, demotivation, reduced effort, annoyance, and, in extreme cases, work disruption. Equity theory suggested that individuals, be it the general public, employees or customers, perceive themselves as either under-

rewarded hence experience distress. This distress however, compels the individual to restore equity or at least recover the perceived losses.

In light of the above, the notion of the equity theory draws from the exchange, departure and social comparison theories in making predictions about managing relations amongst individuals (Adams, 1963). Equity theory focused on the effort on input against the expected outcome from an individual's effort. Naturally, employees compare inputs they offer in terms of labour and expertise with outcomes they receive for their efforts and so are policyholders in insurance (Al-Zawahreh, 2015). The theory assumed that individuals are sensitive to equity; the general preference is that input and outcome, ratios should be equal. Employees and customers tend to also compare the output with that of other service providers (Carrell & Dittrich, 1978; Walster & Berscheid, 1978). Human resources professionals have lately considered the equity theory, especially regarding the fairness of outcomes, attempts to maintain fairness by comparing the inputs and outputs amongst individuals for the same behaviour be it in employment or service delivery. The non-existence of differences between these inputs and outputs is perceived to be equal (Al-Madi, 2012). However, inequity exists when one perceives a disparity in the ratio between input and outcome compared to that of others (Miner, 1980). Inequity exists, according to Adams (1965), when the ratio of outcomes to inputs is uneven to that of others. The equity hypothesis focused on an individual's perception of what existing, regardless of whether being true or not. The individual's perception of the link between inputs and outcomes determines the equitability or inequity (Adams, 1965). According to Adams (1965), inequitable or injustice created dissatisfaction, anger, and guilt. Perceived unfairness by policyholders in the insurance industry was a significant component that triggered customer insurance fraud. Hefty insurance premiums which are currently being deducted from low-income earners directly affect the decision of a policyholder with regards to engaging in acts of insurance fraud considering that policyholders always compare with what other policyholders are receiving from other insurance companies (Insurance and Pension Commission, 2019). Policyholders who perceived inequitable ratios viewed insurance fraud as an acceptable practice (Tseng & Kuo, 2014) and this enhanced policyholders, organised crime syndicates connivance to engage in any form of insurance fraud (Miyazaki, 2009). However, when examining insurance fraud via Adam's equity theory, the premium deduction is not the only factor that must be considered, other contractual factors such as the quality of service delivery need to be considered in

comparison with other insurance service providers. This reduces customers' intention to engage in fraudulent activities.

Furthermore, research has shown that negative behaviours of one employee can spread to the actions of others in the workplace due to peer effects. The crux of the issue may be traced back to Adam's equity theory of job motivation, which was published in 1963. In comparison to others, Adam's notion was about a fair relationship between performance and incentives. It could be argued that the equity theory is not only about remuneration, but also about employee compliance vis-a-vis non-compliance with policies, procedures, and processes. This can lead to a breakdown in teamwork and a general shift toward non-compliance, which can persuade corrupt employees who are more likely to commit insurance fraud if they are employed by insurance companies. A "lone wolf" salesperson or a technical specialist (financial, engineering, etc.) who does not follow or circumvent policies, procedures, and processes, and whose undesirable activities are overlooked due to their perceived importance, are typical instances. When this happens, a team's motivation and morals are severely harmed. When discussing the equity theory, it is important to distinguish between it from the expectancy theory, as the two are frequently confused. According to the expectancy hypothesis, people will be motivated if they believe their efforts will result in the desired outcome. The expectancy theory and the equity theory both take a cognitive approach to motivation, detailing how people change their behaviour, motivation when they believe their efforts will produce results that meet their expectations. People, it is supposed, assess the costs and benefits before making a decision (Stecher & Rosse, 2007). Individuals are driven in both circumstances when they believe their efforts will result in a desired reward, such as money or notoriety. In both cases, we evaluate the valence of incentives; employees will be less motivated to change their behaviour if they do not believe their efforts would be rewarded (effort-reward connection). The equity hypothesis, on the other hand, examined the process of comparing outcome-to-input ratios, as well as the cognitive and behavioural mechanisms that help restore equal attitudes (Stecher & Rosse, 2007). Employees altering their inputs to match their outputs and attempting to modify their outcomes to meet their inputs are two of the ways investigated. People, as predicted by the theory, respond to unfairness by reducing their work effort to match the consequence, but with high possibilities of occupational fraud once the opportunity exists, occupational fraud in these cases is meant to compensate for the perceived losses or imbalances (Stecher & Rosse, 2007).

3.4 Theory of Reasoned Action

The theory of reasoned action is one of the influential theories in examining and causes of fraud. A person's behaviour is determined by their purpose to undertake the behaviour, which is determined by their attitude toward the behaviour and subjective norms, according to the theory of reasoned action (TRA) (Fishbein & Ajzen, 1975). The theory of reasoned action (TRA) is a widely used human behaviour theory that originated in the field of social psychology (Fishbein & Ajzen, 1975). This theory, the theory of reasoned action or attitude towards behaviour, is defined as "an individual's positive or negative feelings (evaluative effect) about performing the target behaviour" (Fishbein & Ajzen, 1975) and "the person's perception that most people who are important to him think he should or should not perform the behaviour in question" (Fishbein & Ajzen, 1975). Both of these dimensions are thought to positively influence behavioural intention to execute certain behaviours, while behavioural intention is thought to positively influence actual behaviour. The idea of reasoned action has been shown to be capable of predicting any human behaviour in a variety of disciplines. In this context, accounting study has used the theory of reasoned action. To the idea of reasoned action, Ajzen (1991) introduced the construct of perceived behavioural control, which was defined as "the perceived ease or difficulty of completing the conduct". This supported the hypothesis that people's behaviour is substantially impacted by their confidence in their ability to accomplish a task (Bandura, 1977). This idea has been used in a number of studies, including those looking at unethical and dishonest financial reporting, as well as forecasting tax fraud and corporate fraud (Malimage, 2019). The theory has served as the foundation for a variety of behavioural theories in a variety of fields. The relationship between behavioural intention and actual behaviour performance, on the other hand, has sparked a lot of discussion among scholars. Behaviour performance is considered a function of intentions and behavioural control as long as the intentions and perceptions of controls assessed are related to the behaviour of interest, and there are no intervening events that affect the intentions and control within the interval between assessment and observation of the behaviour (Ajzen, 1991). Due to the difficulty of witnessing and measuring actual behaviour, most studies have relied on behavioural intention as a proxy for actual behaviour (Warkentin et al., 2012). Several researchers have gathered self-reported actual behaviour to get around this intention-behaviour relationship (Crossler, 2010; Liang & Xue, 2010).

The Theory of Reasoned Action (TRA) when published by Fishbein and Ajzen (1975) was meant to better understand health habits. However, theorists recognised and recommended that the theory should be stretched and applied in any context to better understand and anticipate human behaviours in any economic sector. According to the researchers, behavioural intention can predict the performance of "any voluntary act" unless the intention "a change prior to the performance or the intention measure does not correlate to the behavioural criterion in terms of action, target, context, time-frame, and or specificity." According to the Theory of Reasoned Action (TRA), if an individual's behavioural intention is consistent and the conduct is properly described, a measure of behavioural intention can predict whether or not they will commit a given act. When widening the scope of the Theory of Reasoned Action (TRA), Fishbein and Ajzen's (1975) structure was not completely followed or adhered to. Based on a study of eighty-seven (87) prior empirical studies, they used the theory in situations where the individual did not have full volitional control over the conduct and or where individuals did not have all of the information needed to construct the intention. Surprisingly, they discovered that the Theory of Reasoned Action (TRA) may be effective even when the three basic principles and conditions of the theory were not met properly.

The Theory of Reasoned Action (TRA), like any other theory, has limitations and, like any other theory, needs to be developed and revised throughout time, especially when it comes to choices and objectives. The distinction between a goal intention and a behavioural intention involves one's ability to achieve one's purpose, which is complicated by various variables and thus ambiguous. According to Ajzen (1975), some activities were more likely than others to generate control concerns; hence there is no way to know for sure. When seen in this way, it becomes evident that every intention is a goal whose fulfilment is uncertain. Theory of Reasoned Action does not take into consideration the fact that some conditions that permit the performance of behaviours are not available to individuals. The Theory of Reasoned Action's ability to predict actions that require access to certain opportunities, abilities, conditions, and or resources is restricted because it concentrates on behaviours that people firmly implement. Furthermore, precise intentions do not always play a role in the relationship between attitudes and conduct. According to Bagozzi and Yi's (2000) research, strong intent does not always precede the conduct of behaviour. In truth, intentions are not

necessarily linked to attitudes and behaviours, especially when the conduct does not involve a lot of thought.

Triandis (1979) advocated that the Theory of Reasoned Action be expanded to cover more elements, for example, habit, facilitating conditions, safety and emotion. A habit is formed when a person repeats behaviour on a regular basis, such as criminal acts like fraud. Conditions that make it easier or harder to complete a task are known as facilitating conditions and the safety of the action considering the consequences once compromised. These factors have a direct impact on behaviour, particularly criminal behaviour. Affect, on the other hand, is a person's emotional reaction to behaviour, and this emotional reaction merely influences behavioural intention rather than directly influencing behaviour. Ajzen (1985) expanded the Theory of Reasoned Action to what was then known as the theory of planned conduct in 1985. One key predictor, known as perceived behavioural control, is added to the equation. This amendment was made to account for situations in which persons intend to engage in an activity but are unable to do so due to subjective and objective factors. According to the idea of planned behaviour, a person's attitude, subjective norms, and behavioural control all have significant but differentially weighted influence on their intention to behave. Despite the progress, it is proposed that Theory of Reasoned Action can only account for the determinants of behaviour when motivation and the ability to comprehend information are both high. It is evident that more study is needed to show the causal linkages between the variables in Theory of Reasoned Action and any expansions of it. The memory process is likewise barely mentioned in the model.

3.5 Rational Choice Theory

The behavioural revolution in American political science in the 1950s and 1960s, which tried to explore how people behaved using empirical methods, is said to have spawned rational choice theory (Ogu, 2013). Rational choice theory has applications in a variety of domains, including economics, psychology, and philosophy. According to this theory, people use their self-interests to make decisions that benefit them the greatest, typically financial gain by organised crime syndicates targeting micro insurance service providers and low income earners. According to this view, people use logical calculations to make rational judgments and achieve outcomes that are in line with their own personal aims. An individual makes decisions by weighing the costs, risks, and rewards of several options. Because these decisions are founded on personal preferences, decisions that appear unreasonable to one

person may make sense to another. Rational choice theory is based on the idea that people are in charge of their own decisions. Rational choice theory can aid in understanding individual and group behaviour such as organised crime syndicates, as well as determining why people, groups, and society make various decisions based on specific costs and rewards. An inquiry into the nature and causes of the wealth of nations, written by a philosopher and economist Adam Smith inspired the rational choice theory (Smith, 1776). People analyse their options and choose the option that they believe will best serve them. When examining the rationale behind organised crime syndicates engaged in criminal behaviours and why individuals in an organised crime syndicate conduct themselves in a manner that potentially puts their lives, wellbeing at risk, injury arrest and subsequent imprisonment, the rational choice theory is a theory for understanding individual behaviour. Gary Becker, a 1992 Nobel Prize Laureate in Economics Science and one of the first to apply rational actor models more generally, the rationale for committing a crime is based on a comparison of the rewards and costs of unlawful behaviour (Ogu, 2013). The essence of rational choice theory is that, when a person is given numerous options, he or she usually chooses the one that is perceived to have the best overall outcome (Elster, 1989). In this sense, a member of an organised crime syndicate is seen as a free agent, capable of making rational decisions in practically every area of their lives. The rational choice theory's definition of 'rationality' is more particular and narrower, implying that an individual act as though considering costs and advantages to arrive at an action that maximises personal advantage (Friedman, 1953). Hence, the criminal's decision to commit a crime is therefore based on a "pleasure, pain" principle (Gary & Potter, 2017). If pain is the outcome of an offence and is perceived to be outweighed the reward of committing the crime, this is likely to entice the individual or the whole criminal syndicate to commit the crime. Furthermore, the theory expands that the individuals in an organised crime syndicate do also carry out a risk assessment to consider the risk of detection in comparison with the reward of completing the act successfully. Organised crime syndicates engage in illegal activities for a variety of reasons, including political, religious, economic, psychological, and social motivation (President's Department Intelligence Brief 2020). However, in organised crime syndicates, financial incentives play a significant part in a person's decision to commit a crime (Gary & Potter, 2017). According to Ogu (2013), rational choice theorists make three following assumptions:

- 1) Individuals are expected and ultimately responsible for their acts and decisions.

Individuals, as agents in society and across the world, always behave and act to their

best interest, as rational beings, self-calculating, self-interested, and self-maximising. These individual social acts are the ultimate source of bigger social results. The four other major assumptions summarised are derived from this first overarching assumption.

- 2) Optimality describes how people pick their activities in the best possible way, taking into account their personal preferences as well as the opportunities and constraints they face. According to Abell (2000), optimality arises when the individual preferred no other route of social interaction over the course of action chosen. This is not to say that the actor's course of action is the best in terms of some objective, third-party assessment. The rational choice hypothesis, according to Abell (2000), asserted that people do the best they can, given their circumstances as they see them.
- 3) According to Abell (2000), structures and standards dictated a particular course of action and are just special examples of rational choice theory. In other words, in other cases, the variety of options available varies from those available in a strong structural scenario, where there may be just one option. Individuals will frequently discover a better way to carry out their actions; hence the rational choice model may not always exhibit harmony, unanimity, or equality in their actions. Again, structures as we know them may not be ideal from the standpoint of someone with limited resources, but the rational choice technique will attempt to explain how this scenario originates and is maintained by logical decisions.
- 4) The assumption of self-regarding interest states that an individual's actions are only motivated by his or her own well-being. Although this is an important assumption in the rational choice approach, it is not as important as the assumption of optimality, according to Abell (2000). Other types of communal attitudes, such as collaboration, selflessness, and compassion, may exist, according to Abell (2000), despite the fact that they appear to be at odds with individual optimality at first glance.
- 5) The assumption of rationality appears to be the most widespread in rational choice theory. Everyone acts in ways that benefit them the greatest, according to this notion. This means that everyone is more inclined to take actions that they perceive to be the best possible option and one that will benefit them the most.

Ogu (2013), the rational choice theory has been lauded as the prototype for a more deductive approach to political analysis. Becker (1976) described the rational choice model as a "single

framework for explaining all human behaviour," while Rogowski (1997) described it as the "most rigorous and most general account of social activity that has been created in this century." Hirshleifer (1985) described the notion as "universal grammar of social science". In that line, there are a number of further advantages to the rational choice theory, which can be summarised as follows:

- Generality means that any collection of structural assumptions about the environment in which the actor is present is compatible with a single set of assumptions about each type of actor in a given context.
- Rational choice theories can treat variations in choices among actors and by an actor over time as entirely a function of their structural position when the rational optimisation model is combined with the common knowledge of rationality assumption, the assumption of isomorphic and self-regarding utility function. When selecting what to do, preferences and opinions are simply seen as the sole factors to consider.
- Predictive, rational choice theory assumptions have been used to generate a wide range of definitive theories, whose predictions regarding measurable real-world occurrences rule out a considerably greater set of outcomes than what is currently considered unlikely. The effectiveness of rational choice theories is determined by both structural and individual actor assumptions.

3.6 Deterrence Theory

Deterrence theory proponents argued that people decide whether to comply or break the law after weighing the benefits and consequences of their conduct. Overall, however, proving the effectiveness of deterrence is challenging because only those offenders who are not deterred come to the attention of law enforcement. As a result, we may never understand why others do not offend. The threat of punishment, according to criminology's deterrence theory, will prevent individuals inside an organised crime syndicate from committing a crime, lowering the level or likelihood of offending. Rehabilitation, denunciation, revenge, and incapacitation are the other four goals that punishment is considered to achieve (Dutton, 1999). The first is that specific punishments will deter or prevent a particular criminal from committing more crimes, and the second is that public knowledge that certain crimes will be punished has a generalised deterrent impact that prevents others from committing crimes. Various theories suggested that crime can be reduced by deploying effective counter and or deterrence

measures. The ultimate objective of deterrence, crime prevention is based on the assumption that criminal syndicates or potential criminals will carefully reconsider and re-evaluate the likelihood of being compromised before committing a crime. The deterrence theory rule is that deterrence of a crime such as insurance fraud is both general and specific. The general deterrence theory believes that the prospect of punishment can prevent crime, whereas the specific deterrence theory holds that criminal sanctions should be targeted and harsh enough that convicted criminals will not repeat the same act. The deterrence theory states that credible punishment from a credible and well-enforced criminal justice system, as well as law enforcement agents, will reduce crime by discouraging people from becoming criminals in the first place, continuing criminal behaviour, and even joining an organised crime syndicate. The assumption that both national and international judicial systems prevent crime is the basic basis for their creation and maintenance. Individuals should consider crime to be costly since it entails the possibility of public arrest, conviction, and penalty. The hoped-for result is rational if the threat of punishment is sufficiently certain and harsh (Gary & Potter, 2017).

Western criminal law and criminal justice systems considered that the deterrence concept remains a vital intellectual underpinning. Penal sanctions in death sentence cases and other areas of criminal sentencing have been influenced by the belief that punishments deter criminals. The idea of deterrence that evolved is based on three distinct elements, namely severity, certainty, and rapidity. It is believed that the harsher the punishment, the more likely a rationally calculating human being will refrain from unlawful conducts. As a result, in order to deter crime, criminal law must emphasise sanctions in order to urge citizens to follow the law. Punishment that is excessively harsh is unjust, yet punishment that is insufficiently harsh will not prevent criminals from committing crimes. Punishment certainty basically means ensuring that, whenever a criminal act is committed, there is a penalty. Classical philosophers believed that, if people are aware that their bad behaviour will be punished, they will refrain from doing it again. Furthermore, in order to prevent crime, their punishment must be fast. The closer the punishment is applied to the time of the act, the more likely it is that criminals will discover that crime does not pay. In short, deterrence theorists believed that, if punishment is severe, specific, and rapid, a rational individual will weigh the benefits and drawback before committing a crime, and will be discouraged from breaking the law, if the loss outweighs the gain. Classical philosophers further believed that certainty, rather than the severity of punishment, was more successful in deterring wrongdoing. They condemned

torture as a way of extracting confessions, as well as the death sentence as a viable option for punishing murderers and other violent criminals. The state's fair powers do not extend to capital punishment.

Because deterrence concept underpinnings are occasionally used in criminal justice systems, criminological research continues to discuss the deterrent impact of punishment. The deterrence hypothesis is still being used in programs like boot camps for young offenders and "scared straight" programs. Evidently, various countries have adopted the "tough on crime" policies which were focused on the real and threatened incarceration of criminals. In order to gain additional empirical evidence, criminologists were expanding deterrence notions beyond certainty, severity, and timeliness to incorporate informal social processes such as reward and moral convictions. Deterrence theory has been changed and broadened to include rational choice viewpoints, as some components of deterrence and rational choice theories are part of the routine activities theory. In conclusion, support for deterrence theory is substantially higher now than it was two decades ago. However, research shows that current criminal justice practices place a higher priority on the severity of punishment than on certainty. Death penalty, longer prison sentences, three-strikes laws, mandatory sentencing, and a slew of other "tough on crime" policies have not shown to be more deterrent than less severe penalties. Indeed, increasing the severity of punishment may actually increase crime rather than diminish it. Increases in the certainty of an offender's conviction and punishment, on the other hand, have been proven to have possible implications on crime reduction. Given the background, an attempt by governments to at least come up with policies and legislation that prescribes how criminal conduct such as insurance fraud will be handled and a possible prescription of the penalties is a deterrent measure. However, prescription of lax legislation and penalties on cases of insurance fraud is rather unjust to insurance companies and policy holders. Further, this entices criminal groups to target field which are rather high paying with least risks (Insurance and Pension Commission, 2020).

3.7 Chapter Summary

The literature review chapter of this study dissected across diverse literature, a thorough summary of prior research on particular subjects from insurance, security intelligence, crime and fraud. The literature review examined scholarly articles, books, and other sources that were pertinent to this study. The goal of a literature review was to get a better grasp of the existing research and discussions on a specific topic or field of study, and to provide that

information in the form of a written report. Primary target was to have an understanding of the anatomy of crime and factors that possibly enhance or discourages individual or organised crime groups to commit crime. This rather serves as a departing point in recommending counter measures. It is imperative at this stage to note that the literature review's goal of this study was to summarise and synthesize existing knowledge in a topic without adding any new contributions that distort the meaning. Literature review rather assisted the researcher in even turning the wheels of the research topic because they are based on prior information. Overpowering previous findings required a deep understanding of the research questions and objectives in detail. For other studies, the literature review indicated the path in which they should proceed in order to be successful and as well as informing and refocusing subsequent chapters to issues that are in sync with the research objectives. In that line, the next chapter will dwell on the research methodology. The research methodology discusses how the research subject was conducted by providing a detailed discussion of the research design and methodology.

CHAPTER FOUR

RESEARCH METHODOLOGY

4.0 Introduction

The research methodology chapter of this study entails the research design, research approach and strategy deployed to address the research problem so as to meet the research objective. Research is a systematic examination that employs well-established scientific methods to address or solve problems and develop new, widely applicable information. Systematic observation, classification, and interpretation of data are all part of scientific procedures. Rajasekar et al. (2006) defined research as the systematic and deliberate quest for evolving, most recent and pivotal knowledge on a certain topic. It is rather a study of objective and methodical investigation of scientific and social problems with the goal of developing solutions. Year after year, numerous research investigations are done, undertaken, and completed by a variety of researchers with varying backgrounds and disciplines. According to my observations, an essential aspect of research, particularly research methodology, receives very little attention in the majority of cases. As a result, much research, particularly in the social sciences, comprises a lot of word-spinning, a lot of quotes, and a lot of grey regions. As a result, a lot of study is usually fruitless. In the context of planning and development, it's worth noting that the importance of research is determined by its quality rather than its quantity. As a result, persons involved in research must pay close attention to creating and following appropriate technique throughout the research process in order to improve the quality of the results. While the methodology may differ from one research problem or topic to the next, the basic research strategy remains the same.

This study's research methodology was based on the preconceived concept that research is an academic activity, a scientific study that follows scientific procedures that entails defining and redefining problems, formulating hypotheses or suggested solutions, collecting, organising, and evaluating data, deducing and reaching conclusions, and finally testing the conclusions to see if they fit the hypothesis (Kothari, 1990). According to Kothari (1990), research is an original contribution to the current pool of knowledge with the goal of developing it through study, observation, comparison, and experiment in the pursuit of truth, comparison and deductive reasoning. The "how" part of the study, which is the methodical and scientific technique to answer a research problem by clarifying how a study was carried

out. The methods and tools used in performing the investigation, is referred to as research methodology. Though each research study has its own distinctive goal, according to Kothari (1990), research aims can be divided into four categories:

- i) To gain an in-depth familiarity with a phenomenon while achieving new insights into phenomenon (studies with this object in view are termed as exploratory or formulative research studies);
- ii) To portray accurately research findings, characteristics of a situation or a group (studies with this object in view are known as descriptive research studies);
- iii) To determine the frequency with which something occurs or with which it is associated with something else (studies with this object in view are known as diagnostic research studies);
- iv) To test a hypothesis of a causal relationship between variables (such studies are known as hypothesis-testing research studies).

However, according to Neuman (2014) depending on whether it is quantitative or qualitative research, the approach for planning and performing a study can differ from individual to individual. The research methodology chapter of this study commences by discussing the philosophical worldview of the study and the guiding research design. Hence, this chapter outlines the various stages of research, which comprises the research approach of defining the population of the study, the sampling methodology, and sample size determination, followed by a discussion of the data collection apparatus which assisted in addressing the research objectives. The literature review informed of the research gaps of previous studies, an insight into the causes of insurance fraud, the state of counter measures and the role of security intelligence in countering insurance fraud. Information gathered from the literature review informed the designing and formation of the questionnaire, particularly probing questions that addressed the research questions. Following the questionnaire formulation, the approach to data analysis is explained as well as steps taken to ensure that the research results were reliable and valid. The final conclusive section of this chapter discussed the ethical issues and considerations undertaken in conducting the study.

4.1 Research Philosophy

Research philosophy relates to a system of norms, values and expectations of researchers regarding knowledge creation. Researchers in some instances make conclusions about the

truth of science and human knowledge. It is imperative to note that the nature and manner in which researchers' think and their beliefs can affect the research process (Lewis & Thornhill, 2019). It is the view of Creswell and Creswell (2018) research should be conducted following a clear and defined research approach, that is, a study strategy or roadmap involving the convergence of the research philosophy, the study design, and research methods. Figure 4.1 below demonstrates the inter-relationship between the three key concepts. There are various philosophical worldviews that form the basis of research; the prominent modern schools of thought are the post-positivist and constructivist philosophical paradigms. The post-positivist and constructivist paradigms are very distinct philosophically, but the two can be used together in one research study. If the two paradigms are merged such that one paradigm sets the way for the other paradigm or contributes to the other, the approach is called a mixed approach (Gliner, Morgan & Leech, 2017:10).

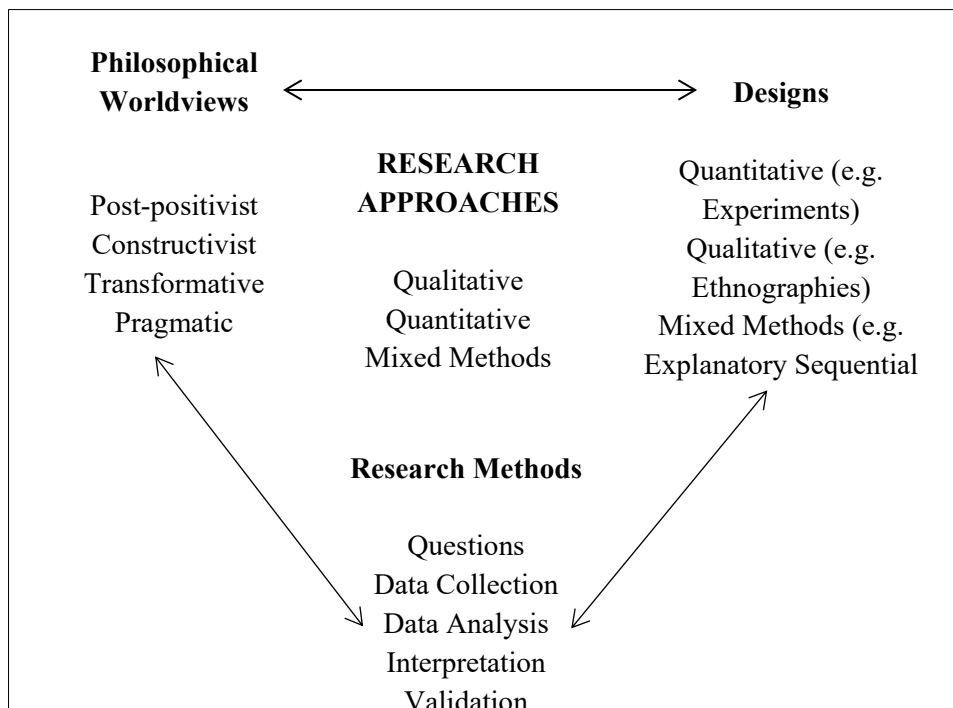


Figure 4.1: A Framework for Research—the Interconnection of Design, and Research Methods

(Source: Creswell and Creswell 2018)

The need to recognize and determine the factors that have an impact on findings is reflected by post-positivists. This approach is reductionist in nature as the goal is to simplify concepts into distinct variables that can form study hypotheses to be tested in addressing specific

research questions. The interpretation that emerges from a post-positivist perspective involves observation and analysis of the empirical realities that exist in the world. The development of numerical measurements of observations and the study of human behaviour is therefore important for a post-positivist perspective (Creswell & Creswell, 2018). This leads to the paradigm being more quantitative in nature (Creswell, 2014). The dominant research paradigm for much of the twentieth century was positivism; this has been largely replaced by a post-positivist philosophical view (Gray, 2017).

On the other hand, constructivism is usually regarded as an approach to qualitative analysis (often paired with interpretivism). The aim of the research is to put as much faith as possible in the viewpoints of the participants on the topic being examined. The questions are broad and generic such that the participants can create a situational context and provide their own analysis and interpretation typically based on discussions. The more open-ended the questioning, the better, as the researcher is able to gather in-depth and rich information on the subject under research (Creswell & Creswell, 2018). The goal of the researcher is to explain the interpretations that others have about the subject under study.

After careful consideration of the research philosophies, the post-positivists approach was the philosophical worldview adopted to answer the research questions for this study. Post-positivist research lays emphasis on inferential statistics with its focus on assigning probabilities that observed findings are correct (Gray, 2017). The study aims to test existing theories, and hypotheses identified in the literature in order to establish a conceptual framework of to counter insurance fraud in the low income sector of Zimbabwe. The objective testing of these theories is to assess the possibility of their generalization and application in the South African farming context. Creswell (2014) suggests that there are rules or ideas that govern the universe, and in order to explain the world, they need to be checked or confirmed and perfected; in this case, these are the low-income farmer's common views, attitudes and beliefs.

4.2 Research Design

The approach is the first step in developing a structure for the research design, and it describes a theoretical model for data collection (Edmonds & Kennedy, 2017). A research design is merely a scientific strategy for investigating a research problem, with the goal of outlining the procedures for collecting and analysing data in accordance with the research

objectives (Grey, 2014). The research design was critical in this study because it allowed the numerous research activities to run smoothly, making the research as efficient as possible and producing nearly accurate data and results. This was a quantitative study, and the research design was critical in translating research objectives into measurable and valid data (Nardi, 2016:7).

This study also conducts a descriptive analysis of the factors influencing the causes of insurance fraud in the microinsurance sector. As a result, descriptive research design aided in the investigation of characteristics or specific criminal behaviour or pattern in a defined population. Descriptive research seeks to predict findings in order to comprehend the various characteristics and to describe the reasons and observations (Joshi, 2019). A descriptive design is used to examine the state of a phenomenon and describe what exists in terms of groups, individuals, or conditions (Edmonds & Kennedy, 2017). Descriptive research is intended to measure what happened rather than why it happened (Gray, 2017). Descriptive research, also known as statistical research, is used to investigate the current situation (Akhtar, 2016).

4.3 Quantitative Research

The goal of quantitative research is to gain a better understanding of the social world. Quantitative methods are used by researchers to observe situations or events that affect people. Quantitative research generates objective data that may be expressed concisely using statistics and figures. Because of the fundamental ideas of post-positivism and deductive logic, this work lends itself to quantitative research methodologies. The deductive approach underpins post-positivist philosophy as a scientific method that emphasises structure, quantification, generalizability, and testable theories (Saunders, Lewis & Thornhill, 2019). Certain research problems, according to Creswell & Creswell (2018), necessitate certain methodologies, such as the identification of factors that influence outcomes; a quantitative approach is the best suited strategy in this regard. Furthermore, quantitative research has the advantage of being efficient in terms of acquiring a high level of involvement, rigorous testing, which is essential for achieving a thorough knowledge of behaviour, and it is also reasonably inexpensive (Jansson-Boyd, 2019).

This study lends itself to quantitative research approaches because of the underlying principles of post-positivism and deductive logic. By analysing the relationship between

factors in this study, quantitative analysis is an approach to evaluating objective theories. In turn, these factors are measured, normally based on survey data from which numerical results are interpreted using statistical analysis. Further, capabilities of quantitative research to tests theories deductively, factoring and guarding against bias, and being able to generalize and replicate the findings (Creswell & Creswell, 2018). In qualitative research, generalization cannot be claimed as results are subject to interpretation (Longbottom & Lawson, 2019), but qualitative analysis enables individualistic data to be collected and evaluated at deeper depths (Mohajan, 2018). As a scientific method that stresses structure, quantification, generalizability and testable theories, the post-positivist philosophy, is underpinned by the deductive approach (Saunders, Lewis & Thornhill, 2019). According to Creswell and Creswell (2018), research problems such as the ones in this study calls for specific approaches such as the identification of factors that influence outcomes; a quantitative approach is the best suited method in this regard. In addition, advantages of quantitative research include efficiency in obtaining great coverage in terms of participation, rigorous testing which is key to achieving a clear understanding of behaviour and it is also relatively economical (Jansson-Boyd, 2019).

4.4 Participants and Sample Size

4.4.1 Participants

A sample size of three hundred and twenty-six (326) research participants. The Taro Yamane method for sample size calculation with a ninety-five per cent (95%) confidence level was used to determine the sample (Uniproject Materials, 2016). According to Mason (2002), sampling is the process of identifying and selecting relevant sources of data, such as people and organisations, as well as providing justifications for the choices made for a study. On that note, sample size determination is the technique to decide on the number of research participants to include in a sample (Singh & Masuku, 2014:6). Sample size depends on different factors, such as the time component, the expense component and the degree of precision needed for the topic under investigation (Dubey, Kothari & Awari, 2017). The three hundred and twenty-six (326) research participants were mainly drawn from regulated micro insurance service providers, the IPEC, low income earners policy holders and the Zimbabwean security intelligence community which comprise the President's Department, Zimbabwe National Army, Military Intelligence Directorate and Zimbabwe Republic Police, Internal Security Intelligence. In qualitative research, selecting an appropriate sample size is a

topic of conceptual debate and practical ambiguity. Experts in qualitative research say that there is no simple answer to the question of "how many", and that sample size is determined by a variety of criteria including epistemological, methodological, and practical considerations. Qualitative sample sizes, according to Sandelowski (2013), should be large enough to allow for the development of a "new and richly textured knowledge" of the phenomenon under research, but small enough to allow for "depth, case-oriented analysis" of qualitative data. According to Vishwakarma (2017) the estimation of the sample size is essentially dependent on confidence intervals, meaning, the accuracy needed to approximate rates, proportions and means. In management research, the common confidence level applied is ninety-five per cent confidence level is selected, as is the case in this study, then ninety-five per cent (95%) out of 100 samples will have the true population value; meaning that, survey questions have been asked to the correct population (Taherdoost, 2017). The Taro Yamane formula for determining the sample size is as follows:

$$n = N / (1 + N (e)^2)$$

Where:

- n = is the sample size,
- N = is the population size,
- 1 = is a constant
- e = is the level of precision.
- n = $1774 / (1 + 1774 (0.05)^2)$
- = $1774 / 5.435$
- = 326

Research participants were an integral component of this study. Making guarantees to participants in this research about how their personal information would be protected was one of the most important components of protecting them. This includes safeguarding participants' privacy, maintaining confidentiality, and or allowing them to remain anonymous considering some of them were from the security intelligence community, organisations operating secretly.

4.4.2 Sampling and Target Population

The primary goal of sampling in this study was to select appropriate research participants so that the study's research objectives and questions could be appropriately researched and

answered. This study acknowledged the importance of a well-designed and thoroughly researched sample selection process, and that improper processes could have a significant impact on a study's findings and consequences (Lopez & Whitehead, 2013). Furthermore, the researcher recognised that the study could not include all research participants (Kitzinger, 1994), so the sample size was calculated using the Taro Yamane method with a 95% confidence level to determine a representative of the study population. Because of its numerous advantages and ability to conduct objective statistical analysis, probability sampling was used for this study.

Sampling is the process of extracting a sample from a population (Alvi, 2016). Participants in this study were chosen at random from the general public. The primary benefit of random sampling is that it yields samples that are most likely to accurately represent the entire population. It also allows for the statistical determination of the sample-to-population relationship, i.e. the extent of the sampling error (Neuman, 2014). Furthermore, for good external validity, random sample processes are required (Crano, Brewer & Lac, 2015). Probability sampling also produces a more representative sample, which is a copy of the population and all of its major variables (Gliner, Morgan & Leech, 2017). Non-probability sampling is also known as judgement sampling because it is impossible to calculate the likelihood that each individual will be included in the survey. This method is prone to sampling bias.

In general, sampling allows researchers to collect enough data to answer the study question(s) without polling the entire population, saving time and money. However, sampling differs depending on whether the investigation is quantitative or qualitative. A good sample should be a representative subset of the population targeted for the study, with each participant having an equal chance of being chosen. The terms population and sample are important in study design. A population is a group of people who share some characteristics. A sample is defined as a subset of the population. The sample size is the number of people included in the sample. The more representative the population sample, the more confident the researcher can be in the quality of the results. Sampling yields important research findings. However, sample errors can occur due to differences between a population and a sample. As a result, selecting the best and most practical sample method is critical. Three of the most common sampling errors are, first, when the sample does not reflect the characteristics of the population, resulting in sampling bias. Second, when the incorrect sub-population is used to

select a sample, sample frame errors occur. Third, systematic errors occur when the sample results differ significantly from the population results. This study acknowledges that efficient sampling provides a number of benefits to researchers (Moss, 2019). Knowing where to sample is just as important as knowing how to sample. Some research topics are better suited to the project's objectives than others. Finding participants who are a good fit for the project's goals is critical because it allows researchers to collect high-quality, accurate data in a timely manner. Data quality is a complex and broad concept that is difficult to define precisely. Nonetheless, one of the most basic definitions of data quality is that it is fit for its intended purpose and has a close relationship with the construct or research objectives being measured. Furthermore, the target population refers to all participants who meet the specific criteria for a research study (Alvi, 2016). The study's target population was divided into three groups: low-income earners, employees in the microinsurance sector, and security intelligence officers. Though Zimbabwe has ten provinces, this study further categorised the target population into regions of Zimbabwe namely Northern, Eastern, Western and Southern regions.

Table 4.1: Stratified sample per region

Province	Sample Size
Northern	81
Eastern	92
Western	91
Southern	62
TOTAL	326

Source: Author's compilation

The criteria for selecting research participants were based on real-life experience and knowledge of the issues under investigation. As a result, the responses of these respondents were likely to provide a true reflection on the factors influencing micro insurance fraud as well as inform the design of insurance countermeasures. The exclusion criteria, on the other hand, were designed to ensure that undesirable elements did not participate in this study.

4.5 Data Collection Techniques

Data collection is equivalent to intelligence collection in security intelligence and it is an initial stage that is directed by a need to answer a research question or intelligence requirement. Hence data is a collection of related observations, facts or figures (Dubey, Kothari & Awari, 2017). The data collection process entails defining the research parameters for the study in the form of sampling and recruitment, then collecting data either using structured, semi-structured or unstructured interviews; finally, developing of procedures for data recording (Creswell & Creswell, 2018). Using the same concept, the researcher surveys for potential sources of data. Gliner, Morgan and Leech, (2017) defined surveying as the process by which a researcher obtains data using multiple approaches or some sort of instrument that can be scored numerically and reliably. Four distinct methods were used for data collection in this study, namely survey through a questionnaire, interviews, focus group and document inspection. The questionnaire was deployed as the instrument for collecting the primary data complemented by interviews, focus groups discussions and document inspection (Cohen, 2013). Considering, the diversity and secrecy of data which was required, research participants were grouped into the macro category which comprise the regulatory authority, the Insurance and Pension Commission, regulated insurance companies offering services to low-income earners, intelligence the security intelligence community and finally policyholders (low income earners) mostly victims of micro insurance fraud. This study deployed a hybrid approach in which after the questionnaires were analysed and documents inspected, question for interviews were generated based on analysis and inspections so as to address grey areas and data gaps. Structured, semi-structured, unstructured and focus groups interviews were also done with the four categories. The fact that qualitative and quantitative research requires distinct data and data collection methods, the type of research defines the sort of data gathering strategy to be employed. If the research data is incomplete or incorrectly obtained as a result of a variety of factors:

- It will be unable to respond to the research problem.
- It can have a hard time answering research queries.
- Because the device is unreliable, the research may not be able to withstand the test of time.
- It won't be able to measure the things that are supposed to be measured.
- It will lead to erroneous conclusions.

4.5.1 Questionnaire

The questionnaire was the main instrument for collecting data in this research. A self-administered online questionnaire composed of standardised questions which followed a fixed scheme in order to collect individual data with regards to various issues mainly and related to the research objectives, types and causes of insurance fraud, threat level and socio-economic impact of insurance fraud, modus operandi used by organised crime syndicates to expand their criminal activities, frequency of insurance fraud cases, measures being implemented in the industry to mitigate insurance fraud, profile effective counter measures and assess the role of the security intelligence organisation in countering insurance fraud (O’Leary, 2014). Questions and instructions issued out to the participants were initially designed based on a preconceived idea that the questions should be answered neutrally and objectively irrespective of other questions requiring information of intelligence and security value to be disclosed (Klein, 2003). Stya (2012), Figure 4.3 below outlined the stages of planning that contributed to the creation of a successful questionnaire.

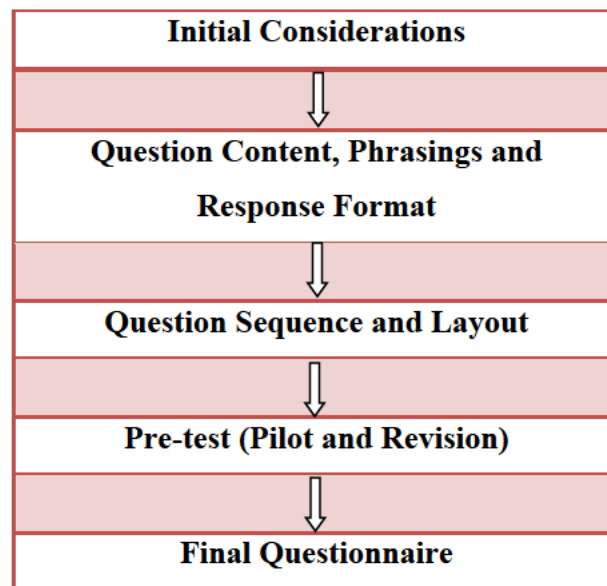


Figure 4.3: Stages of planning a questionnaire

(Sources: Stya, 2012)

A questionnaire frequently includes both open and closed questions. This is advantageous since it allows for the collection of both quantitative and qualitative data. Questionnaires allow for the gathering of both subjective and objective data from a wide sample of the study population in order to generate statistically significant results, which is particularly useful when resources are restricted. Further, in line with this study, questionnaires are an effective

method for safeguarding the participants' privacy. Complementary to Debois (2022) the deployment of the questionnaire in this study had numerous advantages namely:

- i. The use of the questionnaire was cost-effective. Self-administered questionnaires, in particular, were a cost-effective approach to swiftly collect vast volumes of data from a big number of individuals in a short period of time without having to engage third parties or research assistants to do face-to-face interviews on behalf of the researcher;
- ii. An option to post the questionnaire on website or send it to the participants via email or administered on mobile phones also existed. These approaches are low-cost or free; however, precise targeting was required in order to get highest response rate and the most accurate data;
- iii. Apart from being inexpensive, the questionnaire was also a practical way to gather data. They can be targeted at certain populations and handled in a variety of ways. The researcher has complete control over the questions asked and the structure be it open-ended or multiple-choice questions;
- iv. The questionnaire provided a technique to collect massive amounts of data on this particular topic under study. Furthermore, results were collected quickly and easily using online and mobile applications. Depending on the volume and reach of inquiry, insights were obtained in as little as 24 hours or less;
- v. The questionnaire allowed the researcher to collect data from a big group of people and the collected data was easily quantified and made it easy to compare and contrast with other studies as well as to track changes. Improving comparability necessitated the reduction of translation errors; and
- vi. The majority of survey and questionnaire providers were quantitative in nature, allowing for straightforward results interpretation.

4.5.2 Administration of the questionnaire

It is only when questionnaires are adequately designed and administered in a responsible and consistent manner that vital conclusions can be drawn about specific groups and the population under investigation (Roopa & Rani, 2012). The environment created by quantitative data gathering allows for the collection of the most data possible while adhering to resource and time restrictions by allowing one data collecting method's strengths to outweigh its weaknesses (Dillman, Smyth & Christian, 2014). The questionnaire was

administered through a mixed-mode combination of a telephonic and self-administered online questionnaire. For survey enquiries, the single mode model, which means that one data collection mode suits all participants, is no longer tenable (de Leeuw, Suzer-Gurtekin & Hox, 2016:2). By using various types of data collection methods, a researcher can enhance the validity and reliability of the collected data. Respondents to this study were informed initially by email then followed with telephone, notifying them of the study, requesting their participation and advising on the date and time to expect to be issued an online link of the questionnaires. On the agreed date, short message services (SMS) were sent to the participants a day before, making reference to the previous email and telephone conversations requesting the participant to make time the following day. Participant in the security intelligence required a one-week security clearance to respond or answer the questions sent to them hence for these a request was sent two weeks in advance.

Of all survey techniques, telephone surveys are the most often utilised (Gray, 2017). The questionnaire was well-complimented by follow-up telephone interviews, which were more effective due to the targeted study participant's estimated 79% cell phone penetration rate. The researcher's ability to obtain real-time clarity on grey areas through response rate telephone interviews helped to reduce response selection errors since the interviewer had control over the process of selecting potential responses (Stoppa & Rani, 2012). The global health emergency brought on by the corona virus (Covid-19) pandemic also played significant a role in the planning for a research design. In order to limit and slow the spread of the virus, the government of Zimbabwe, through its responsible ministry, the Ministry of Health and Child Care established tight travel restrictions within provinces and mandated that residents stay at home as much as possible. Face-to-face interviews were therefore deemed to be high risk in the planning of the data collection strategy due to government restrictions and in accordance with safety precautions. Mailing of questionnaires was also not considered due to postal service disruptions during the pandemic and the risk that the questionnaire might not reach the intended participant in a timely manner. As a result, it was determined that telephone interviews and online surveys were practical and best choice for data gathering. In cases where research participants had a good internet connection virtual interviews and focus group discussions were done online.

4.6 Test Run

Prior to gathering actual data for the study, a formal process known as a "test run" was used to collect data with a sample that is comparable to the planned research study. This step is crucial for demonstrating the reliability and validity of the research findings and alerting the researcher to any necessary adjustments (Gliner, Morgan & Leech, 2017). The test run is a crucial part of a study that helps reduce needless work by pre-testing the questionnaire, improving the integrity and general quality of the primary research. Removing or at least decreasing items that are likely to be deceptive, intrusive, or just where respondents may not know how to respond, test-running a questionnaire typically streamlines the data collection process and lowers the likelihood of missing data (Gray, 2017).

An experiment was conducted using a sample of twenty randomly chosen respondents, of which five were low-income earners, two were from the Insurance and Pension Commission, three were from Zimbabwe's security intelligence community, and ten were from insurance companies that provide services to low incomes earners and households. However, the researcher set up the test run to be a copy of the real investigation; with participants taking part consciously hence it mirrored the real survey. Research participant were made aware of the research and purpose. Prolr concent was obtained. The questionnaire's questions, format, and scales were all improved in advance of the test run in order to increase respondent comprehension and the questionnaire's overall flow (Crewsell, 2014). According to Nardi (2016), a questionnaire's design elements, such as the way the items are arranged, can also have distinct results that can enhance the calibre of the data gathered. After the test run of the questionnaire was finished, changes were made and the questionnaire's general final evaluation was carried out.

4.7 Interviews and focus group discussions

An interview, according to Kvale (1996), is a face-to-face dialogue with the goal of gathering data in the form of descriptions of real-life situations, experiences, and knowledge of the interviewee. It entails giving the interviewer information about how to understand the meanings of the 'described phenomena' (Creswell, 2012). Similarly, Schostak (2006) used interviews as an extendable conversation between the researcher and the participants with an aim of having 'in-depth information' about insurance fraud, its perpetrators, why is it targeted at low-income earners and profiling possible countermeasures. Besides face-to-face, one-on-one interviews and focus groups discussions were also a remarkable and effective data

collection technique from diversified data sources at one go (Marshall & Rossman, 2006). Given the diversity of the information required for this study, accumulating such data was done in a phased approach. First, the researcher had structured interviews with insurance head of claims departments and members of the Zimbabwean Intelligence Community, whose key features complemented the questionnaire in that it was organised around a set of predetermined direct questions that required immediate responses (Berg, 2007). The contents of the interview were mainly focused on identifying the frequency of insurance fraud, why it targeted insurance companies who offer services to low-income earners and if there are any countermeasures in place as well as having an understanding of suggested possible countermeasures (Gubrium & Holstein, 2002). Unstructured interviews were conducted mainly with regional or provincial insurance managers, senior intelligence and security officers responsible for anti-corruption and officers at the Insurance and Pension Commission. This allowed for an open situation through which a greater flexibility and freedom was offered with an objective to elicit the *modus operandi* used by organised crime syndicates, profile possible solutions that could be effected to counter insurance fraud and possible identify, if an intelligence and security organisation could assist the insurance industry at national level to counter insurance fraud. Thirdly, semi-structured interviews were conducted across the board of participants primarily to gather data and probe for explanations and get practical examples by expanding interviewee's responses (Rubin & Rubin, 2005). Fourthly, focus group discussions with two groups of participants, namely one which comprised employees from various departments of the insurance companies and policyholders who are also victims of insurance fraud and another which comprised Insurance and Pensions Commission Policy and legislation experts, insurance companies risk managers and intelligence and security experts from the intelligence community. The former group highly focused on having a diversified view of types of insurance fraud and *modus operandi* affected by criminals while the later was seized with designing counter insurance fraud measures

4.8 Documents inspection

Documents were an important source of secondary data in this study. Documents included Zimbabwe Republic Police criminal records on insurance fraud both pending and completed cases, intelligence on activities on organised crime syndicates collected by the security intelligence community, recorded statistics on insurance fraud, government legislation, acts

and policies. The researcher had clearance to classified documents with the intelligence and the police. Restriction was only on documents classified as top secret. The Insurance and Pension Commission had also granted the researcher access to other confidential documents in the organisation and insurance companies. Classified documents within the Insurance and Pension Commission, and police and intelligence community were essential in giving intelligence or information leads with regards to types, causes, costs involved, targets and sources of insurance fraud and it was effective in the evaluation of possible countermeasures to combat insurance fraud. Document inspection and analysis is a type of qualitative research in which the researcher examines and interprets documents in order to give voice and meaning to the research topic (Bowen, 2009). Document inspection, evaluation and analysis of the contents of document, collected intelligence in form of audio and documented intelligence briefs and on-going and completed investigations were included in this study because it is a social science research method and an important research tool in and of itself, and it is an essential component of most triangulation schemes, as well as the combination of methodologies in the study of the same phenomenon (Bowen, 2009). Qualitative researchers typically use at least two resources to achieve convergence and collaboration, such as distinct data sources and methods. The goal of triangulating is to create a cluster of evidence that nurtures trustworthiness and accuracy (Bowen, 2009). Analysing and evaluating information obtained using various approaches and correlating findings across data sets, the influence of potential bias can be reduced. Mixed-methods studies, which include qualitative and quantitative data, are sometimes used in document analysis. For research, a researcher can employ a wide variety of texts, but written papers are likely to be the most popular (Bowen 2009). The data gathering strategies used in this investigation are summarized in Table 4.2.

Table 4.1: Data Collection Techniques

	INTERVIEWS					DOCUMENTS
	QUESTIONNAIRE	STRUCTURED	SEMI STRUCTURED	UNSTRUCTURED	FOCUS GROUPS	DOCUMENT INSPECTION
Questions Asked	Same for all participants	Same for all participants	Guided by response, but with interview guide	Guided by response, but with no interview guide	Same questions, but, guided by response, but with no interview guide	Guided by information on the documents, but with a guide on information required
Pre-Determined Questions	Yes	Yes	Some	No, but guided by research objective	Yes, but guided by research objective	Yes
Open Ended Questions	NO	No	Yes	Yes	Yes	No

Question Wording	Standard	Standard	Flexible	Flexible	Flexible	Standard
Typical Use	Collection of fact related to the objectives	Well-developed understanding of the research objectives with clear focus	Other relevant data	Researcher's understanding still evolving	Diversified views of people involved	Historical understanding of the issues in question relating the data to the research objectives.
Data Recording	Filling the questionnaire.	Written and Audio recording	Audio recording and use of note taker for analysis afterwards	Audio recording and use of note taker for analysis afterwards	Audio and video recording combined with a note taker for further analysis.	Photocopying and or photographing and notes taking
Benefits	Fast and cost efficient	Efficient and no rapport required. Responses can be easily compared across respondents	Participants allowed freedom to express their views and provide reliable, comparable qualitative data	Useful if understanding of area not yet established	Diversified views of people involved	Historical data which can be used as evidence.

(Sources: Owners Compilation)

4.9 Research Objectives and Methodology

This part refers back to Chapter (1), where the technique was connected to the research goals. Four key research aims and four research questions were selected in this study. A link with methodology was made to attain the objectives, which effectively answered the research questions that were determined earlier (Silverman, 2010). The connectivity and relationship between the study objectives, questions, and methods is clarified and simplified in Table 3.4.

Table 4.2: Linkage between Methodology and Research Objectives

NO	RESEARCH OBJECTIVES	RESEARCH QUESTIONS	RESEARCH METHOD APPLIED
1	To investigate the causes of micro insurance fraud in insurance companies offering services to low-income earners.	What are the motivators of micro insurance fraud in insurance companies offering service to low-income earners?	Questionnaire Interviews with players in the insurance industry Focus group discussions Documents inspection
2	To evaluate the impact (threat level) of micro insurance fraud targeted at low-income earners to national security and interests.	Is insurance fraud targeted at companies offering services to low-income earners a threat to national security?	Questionnaire Focus group discussions Documents inspection
3	To assess the role of security intelligence in countering	What is the role of a security intelligence in	Questionnaire and interviews with the

	insurance fraud rampant in insurance companies giving service to low-income earners.	countering insurance fraud in insurance companies offering services to low-income earners?	intelligence and security community Documents inspection
4	To prescribe other possible strategies to counter insurance fraud in insurance companies offering services to low-income earners.	What other strategies that can be implemented to counter insurance fraud in the micro insurance market?	Questionnaire and interviews with the intelligence and security community, players in the insurance industry Semi-structured interviews with policyholders Focus group discussions Documents inspection

(Sources: Owners Compilation)

4.10 Data Analysis

4.10.1 Correlation Analysis

The strength and type of links between various variables can be examined, analysed using methods namely correlation and regression analysis. To comprehend the nature of relationships between two distinct variables, correlation analysis was utilized in this study. . In correlated data, the degree of change in one variable is associated with a change in the magnitude of another variable (Schober, Boer & Schwarte, 2018). Structural equation meddling (SEM) usually refers this to causal effect analysis. The degree of association can be between dependent and independent variables, or between two independent variables (Senthilnathan, 2019). The use of the cause and effect analysis helps find all of the potential causes of a problem. The degree of association can be between dependent and independent variables, or between two independent variables (Senthilnathan, 2019).

Correlation coefficient 'r' is calculated through the following formula:

$$r = \frac{n \sum xy - \sum x \sum y}{\sqrt{(n \sum x^2 - (\sum x)^2)(n \sum y^2 - (\sum y)^2)}}$$

Where, x and y are values of variables, and n is size of the sample.

The value of correlation coefficient can be interpreted in the following manner:

If 'r' is equal to 1, then there is perfect positive correlation between two values;

If 'r' is equal to -1, then there is perfect negative correlation between two values;

If 'r' is equal to zero, then there is no correlation between the two values.

Correlation coefficients are used to assess the strength and direction of the linear relationships between these two identified quantitative variables. The results of correlation analysis produce a correlation coefficient which ranges from -1 to +1. A correlation coefficient of +1 show that the two variables are perfectly positively correlated, a correlation coefficient of -1 suggests that two variables are perfectly negatively correlated, while a zero correlation coefficient reveals that there is no linear relationship between the two variables under investigation (Gogtay & Thatte, 2017). Senthilnathan (2019) presents an ideal spectrum for interpreting correlation coefficient results within a range of acceptability.

Table 4.3: Ideal spectrum for interpreting correlation coefficient

Positive	Interpretation	Negative
0 to 0.2	Very weak or negligible correlation	0 to -0.2
0.2 to 0.35	Weak correlation but to be considered	-0.2 to -0.35
0.35 to 0.5	Fair or moderate correlation	-0.35 to -0.5
0.5 to 0.7	Strongly considered high correlation	-0.5 to -0.7
0.7 to 1	Very strongly considered correlation	-0.7 to -1

(Source: Senthilnathan 2019)

Correlation analysis does not confirm that the association between two variables is a cause-and-effect relationship (Schober, Boer & Schwarte, 2018). For the investigation of causal relationships in this study, SEM was used. This is when structural equation modeling is used to simulate potential links between manifest (observed) and latent (unobserved) variables. Structural equation modeling is used extensively in the social sciences, but it is also appropriate for use in other fields like business, ecology, engineering, finance, pharmaceuticals, and research. A structural equation modeling can serve as a structural causal model to facilitate causal inference under certain conditions (SCM). Path diagrams, which are frequently used with SEM, are visual depictions of the postulated dependencies and correlations, and they are especially helpful for examining causation.

4.10.2 Structural Equation Modelling

The data were analysed using SEM specific programme AMOS in SPSS. The association between insurance fraud, organised criminal syndicates, and low-income earners was investigated using SEM. SEM which combines factor analysis with path analysis, is a fairly generic statistical technique that is commonly employed in behavioural sciences. The purpose of SEM was to see if there was a relationship or causal effect between insurance fraud as an independent variable and its linkage to dependent variables such as organised crime syndicates and low-income earners. Structural equation modelling is a dynamic, multivariate approach that is well suited to evaluating different hypothesized or implied relationships between variables (In'nami & Koizumi, 2013). SEM uses various types of models to describe complex relationships between observed and latent variables.

Structural equation modelling is a general linear model (GLM) extension that allowed the researcher to test a number of regression equations at the same time. Traditional models can be tested with SEM software, but it can also examine more sophisticated linkages and models, such as confirmatory factor analysis. The researcher specified a model based on theory before determining how to measure constructs using SEM. The advantage of using SEM is that it models measurement error to produce unbiased estimates of the relationships between variables. Traditional statistical methods including, analysis of variance (ANOVA), multiple regression and path analysis of variance ignore measurement of error variables in a model (Wang & Wang, 2020). The researcher gathered data and entered it into the structural equation modelling software package, which generated outcomes such as overall model fit statistics and parameter estimates (Texas A&M University, 2012).

Structural equation modelling models often comprise two subsets of models: a measurement model and a structured model. A measurement model describes the extent to which the variables observed act as a measurement instrument for the underlying construct. A structured model hypothesizes and assesses potential relationships among latent variables (Wang & Wang, 2020). SEM can be applied both in confirmatory testing and in exploring the construction of new models. It is mostly used as a confirmatory tool to ascertain the validity of a specific model (Rahman, Shah & Rasli, 2015). For the following five reasons, this study deployed the structural equation modelling and confirmatory factor analysis with AMOS:

- i) The statistical analyses' assumptions are transparent and testable, allowing the researcher complete control over the investigation and a thorough knowledge of the results;
- ii) Confirmatory factor analysis with AMOS, and structural equation modelling (SEM), provide overall model fit and individual parameter estimate testing all at once;
- iii) It is possible to compare regression coefficients, means, and variances at the same time;
- iv) To reduce the impact of measurement error on inferred correlations between latent variables, measurement and confirmatory factor analysis models can be employed to purge mistakes; and
- v) Confirmatory factor analysis utilises AMOS' capacity to fit non-standard models, including flexible longitudinal data handling, databases with auto correlated error structures, and databases with non-normally distributed variables and incomplete data.

4.10.3 Reliability and Validity

Reliability relates to the consistency of replies to various data set coders. It can be improved by taking thorough field notes, recording them, and then transcribing the digital data. Validity in qualitative research, however, might be described in a different way than in quantitative research. As the naturalist's version of internal validation, external validation, reliability, and objectivity, Neuman, (2014) employed "trustworthiness" of a study. In qualitative research, credibility, authenticity, transferability, dependability, and conformability all contribute to trustworthiness. Reliability and validity are concepts that establish the truthfulness, credibility, or authenticity of findings (Neuman, 2014). The purpose of establishing reliability and validity in research is essentially to ensure that data collected is sound, replicable, and the results are accurate (Mohajan, 2017). Reliability is a measure of consistency, of which the extent of this consistency is measured by a reliability coefficient using a scale from 0 to 1 where 0 is very unreliable and 1 is perfectly reliable (Gray, 2017). Questionnaires and interview schedules were created keeping the research's target groups in mind. These, presumably, will be suitable to address all difficulties arising from the insurance business, insurance companies, and intelligence and security. Cronbach's alpha was used to assess the questionnaire's overall internal consistency, which included a Likert scale. The Likert scale, which ranged from 0 to 5, and was used to assess the extent to which respondents agreed with the ideas in the evaluation items, and it was assessed using the

method of data collection, while the Cranach alpha was used to assess consistency across industries. The findings revealed that insurance fraud is perpetrated by organised crime syndicates, who target low-income earners, and that there is a need to involve the secret services in combating insurance fraud. NVivo 12 for Windows software, which is ideal for qualitative and mixed-methods research, was utilised for the analysis of unstructured text, audio, video, and picture data, such as interviews, focus groups, and document inspection. The NVivo 12 for Windows software was used to examine initiatives to combat insurance fraud at the industry level, including current fraud detection and deterrence systems, employee anti-fraud culture, low-income policyholder awareness, and fraud cases handling in terms of investigations and prosecution. Validity, researchers most frequently use the general term "validity" to assess the worth or quality (Gliner, Morgan & Leech, 2017).

Validity is the question of what an instrument measures and how accurate it is. It is the extent to which outcomes are accurate or inaccurate (Mohajan, 2017:14). Taherdoost (2016) validity can take many different forms, including face, content, and criteria validity, all of which are further described and represented graphically in Figure 4.4 below.

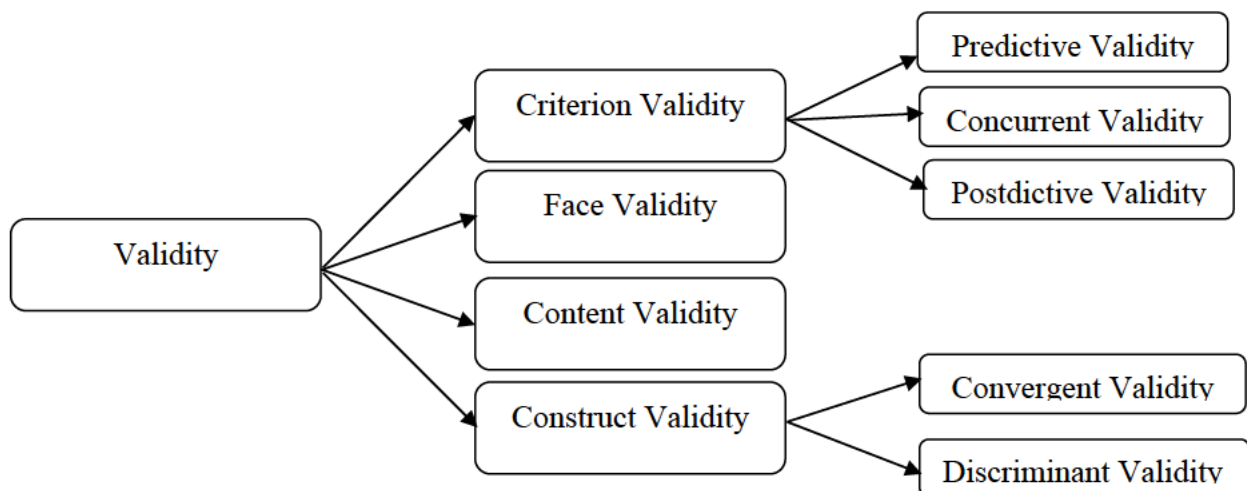


Figure 4.4: Various forms of validity

(Source: Taherdoost 2016)

Construct validity: refers to how well a translated concept or behaviour establishes a construct into a functioning and operating reality, which is the operationalization. Construct validity has two components: convergent and discriminant validity (Taherdoost, 2016). Construct validity was assessed by performing a Confirmatory Factor Analysis (CFA). This

is particularly helpful in identifying the factor structure that best describes the phenomena as observed on the basis of theory. Criterion validity applies to the degree to which particular criteria variables can be estimated by test scores (Taherdoost, 2016). Typically, this validation method requires setting a correlation coefficient between the instrument and some sort of external criteria. Predictive validity assesses the operationalization's ability to predict something that it should technically be able to predict, and concurrent validity assesses the capability of the operationalization to differentiate among classes that it should theoretically be able to separate (Taherdoost, 2017). In qualitative research, "appropriateness" of the tools, methods, and data refers to validity. In order to answer a research question, a methodology must be appropriate, the design must be valid for the methodology, the sampling and data analysis must be valid for the methodology, and the results and conclusions must be valid for the sample and context. For a methodology to be valid, it must be able to identify discoveries or occurrences in the proper context while taking into account cultural and contextual variables. Consultations with various insurance experts and intelligence officers regarding the questionnaire's role in providing feedback on the survey's suitability and reasonableness for assessing what it seeks to,

4.10.5 Bias Reduction

The possibility of bias through questionnaire design exists in every questionnaire (Frey & Pirscher, 2019). Bias refers to the extent to which the researcher or respondents may seek to influence the process of data collection, analysis and findings either wittingly or unconsciously (Longbottom & Lawson, 2019). An understanding of research bias prior research is pivotal and crucial in research for several reasons namely bias exists in any form of research, across research designs and is difficult to avoid or eliminate. Bias can occur at each stage of the research process and impacts on the validity and reliability of study findings consequently misinterpretation of data, distortion of results and subsequently inaccurate conclusions and recommendations (Smith & Noble 2014). Smith and Noble (2014) as according to table 4.5 below identifies five types of research bias:

Table 4.4: Types of Bias

NO	TYPE	DESCRIPTION
1	Design Bias	An inappropriate, poor study design which is not in sync with study objectives and research questions increases the likelihood of bias.
2	Research Participants Bias	Selection bias relates to the process of identifying recruiting participants and study inclusion criteria. Successful research begins with recruiting participants that meet the study aims.
3	Data Collection and Measurement Bias	Data collection bias can occur when a research's personal belief influence the way information or data is collected while measurement bias can occur if a tool or instrument has not been assessed for its validity or reliability is not suitable for its validity or reliability is not suitable for the specific settings or groups.
4	Analysis Bias	When analysing data, the researcher may naturally look for data that confirms their hypothesis or confirms personal experirnce, overlooking data inconsistent with personal beliefs.
5	Publication Bias	Published studies nearly always have some degree of bias and the findings can be applied in other studies.

(Source: Smith and Noble, 2014)

To address the concern of potential bias, the scenario under investigation was explained to study participants in clear and easy language, the issues under investigation, its threat to national security, to the policy holder and the insurance industry. Further the intended use was explained along with the purpose of the research. This gave research participants a better understanding of the study. Also, having a well-designed research protocol explicitly outlining data collection and analysis. Smith and Noble (2014) minimising bias is a key consideration when designing and undertaking research. Researchers have an ethical duty to outline the limitations of studies and account for potential sources of bias.

4.11 Ethical Issues

This study was based on international fundamental human rights and the ethical principles that guide all scientific research. The data which was collected was highly sensitive and of security nature mostly, referred to as “classified intelligence”. Participants in the insurance industry, which is a private sector, expressed concerns about the security of company data,

company practices, and any confidential information relating to clients, while officers in the security intelligence sector expressed concerns about the breach of the "Official Secrecy Act" and the "Need to Know" principle, which prohibits the disclosure of intelligence to third parties. In view of the foregoing, participation in this study was contingent on clearance from the Insurance and Pension Commission, the government's controlling body for the insurance industry, and the President's Department, which is in charge of national security intelligence. Participants participated on the basis of offer by the researcher and voluntary acceptance. Clearance of the participants by their superiors and or their insurance company or organisation was, however, of significance importance.

Prior to data collection, the researcher educated the participants with regards to what the research was all about, its objective and importance of the research. All participants before being issued a consent form were issued out an information sheets, confidentiality form, simplified proposal and letter of authorisation to conduct research. This was a proactive measure to avoid incidences of either a company or organisation to pull out or its participants cancelling the consent form due to issues of sensitivity, confidentiality concerns and time constraints. The confidentiality form was meant to assure the participants that information they disclosed was purely for study purposes and it was not to be used for any other purposes or to be disclosed to third parties who had nothing to do with the study. The four (4) documents (consent form, confidentiality form, simplified proposal and letter of authorisation to conduct research) which the researcher named the ethical pack was issued to participants' prior their participation. This gave the participants an assurance that data or information they were given out was to be handled safely and confirmation that the research was authorised to conduct the research. Furthermore, participants would participate at their own volition. In general, the ethical pack made sure that the research was to be conducted in a manner that is consistent with ethical principles and highest level of confidentiality considering that some of the respondents were in the intelligence and security service and the information they provided was classified. In that regard, the below four areas were clarified to the research participants through the ethical pack and verbally.

- i) **Security clearance:** A consent letter and security clearance was obtained from the President's Department and Insurance and Pension Commission;

- ii) **Informed consent:** Participation was on a voluntary basis and respondents were allowed to withdraw at any time from the survey;
- iii) **No harm to participants:** A brief explanation on the contents of the study and its intended objectives was communicated to the participants; and
- iv) **Need to know principal:** An undertaking from the researcher that information of intelligence and security value and any other relevant information were only for study purpose and would not be disclosed to third parties.

With regards to document inspection and focus group discussions, the researcher had a security clearance to inspect files of cases of insurance fraud being handled by the Zimbabwe Republic Police and files for profiled organised crime syndicates who are under the President's Department surveillance and continuous monitoring target list. The researcher was not allowed to make copies or withdraw these documents. The instruction was "eyes only" classification. The Insurance and Pension Commission cleared the researcher to also have access to cases being handled or invested by insurance companies in their claims or risk management departments. Regarding group interviews, the researcher was granted access to major fraud cases meetings which gave the researcher an opportunity to interact and ask questions with regards to issues related to micro insurance fraud. Furthermore, the researcher was cleared to attend intelligence and security briefings on fraud and corruption. This was made possible with the clearance of the Insurance and Pension Commission and the President's Department. However, the use of recording gadgets was restricted.

Trustworthy and authenticity of the information produced by this study was also pivotal in this study. The credibility of this study was established using Lincoln and Guba's (2000) guidelines, which emphasised that a qualitative study should have an aspect of credibility based on internal and external validity, dependability (it has the quality of reliability), and conformability (is objectively driven). Because of the factors incorporated in the research method through the reporting phases of the study, this study can be assessed to be trustworthy and authentic. It was conducted utilising a scientific case study methodology that allowed the use of a range of sources to validate the results, the study had some credibility. It was carefully constructed using a conceptual framework derived from fraud definition principles applied to difficulties in the insurance sector as a whole. Aside from the case study's methodical principles, the study provided clear guidelines for the research's transferability.

This study passed the validity test because the contents were not generalised, but rather information gathered from sources, and the findings could be used to develop policy or make changes to existing policy and legislation, as well as show the insurance industry how to use the national intelligence and security apparatus to combat insurance fraud perpetrated by organised crime syndicates. This research was highly dependable considering that it profiled practical countermeasures for micro insurance fraud based on information provided by main sources of information most importantly industry players and the regulatory authorities. The industry players or the insurance companies and the regulatory authority, that is, the Insurance and Pension Commission, are heavily affected by the increasing levels of micro insurance fraud. They are in need of such researches. Finally, this study followed the scientific research technique to the letter. The research concept, methods, and procedures were all documented in the descriptions and documentation. It ensured objectivity with the elements and timely feedback from sources that can be regarded as credible in forming any assumptions about the issues at hand.

4.12 Chapter Summary

The research methodology components were pivotal in achieving research objectives of this study. Insurance is increasingly becoming an important component of human security in Zimbabwe and globally (Insurance and Pension Commission, 2019). In that regard, coming up with research based counter measures will go a long way in containing micro insurance fraud in the low income market segment. The relevant sample, sampling process, and inclusion and exclusion criteria were all clearly defined and identified, along with the target demographic that was the subject of the inquiry. This study deployed the methodology techniques and tools that made it possible to gather not just sufficient data but accurate data that was relevant in responding the research questions. The research design was crucial in this study since it allowed the numerous research activities to run smoothly, making the research as efficient, as feasible and generating almost accurate data and outcomes. This study is a quantitative study with a mixed method approach. Mixed method approach was selected on the need to combine both quantitative and qualitative methods. Data was gathered using four (4) different techniques: questionnaire surveys, interviews, focus groups, and document reviews or inspection. The questionnaire was deployed as the instrument for collecting the primary data. However, in the insurance and security sector data was classified and restricted. The research tools deployed were however able to tap into even restricted data in both the

insurance industry and the intelligence and security sector. Ethics were considered during the data gathering process, and the study was supported by ethical conduct guidelines. In order to contextualize debates and discoveries, the next chapter included analysis and interpretation of the data that was gathered utilising graphs, charts, and tables as well as literary references. Conclusions from the data were also drawn utilising a number of statistical tests and methodologies to address the research questions and objectives offered in this study.

CHAPTER FIVE

DATA ANALYSIS

5.1 Introduction

The data analysis and research findings are an analysis, discussion and presentation of the data collected to address the research problem and objectives set forth in Chapter One (1). The research design of this study was conducted in sync with the research problem, questions and objectives with a preconception to outline the procedures for gathering data, analysing the data and presenting it in light of the study's objectives and questions (Neuman 2014). The presentation and interpretation of empirical findings, as well as the analysis of collected data, are detailed in Chapter five (5) of this study to address the research questions and objectives set forth in Chapter one (1). Data interpretation, according to Neuman (2014), entails creating charts, tables with frequencies and percentages, and descriptive statistics, as well as inferential statistics, in which the data is analysed to determine the underlying meaning, using knowledge of the research topic and drawing on the existing body of theory to best represent the data to respond to the research objectives. A questionnaire, interviews, focus groups, and document inspection are among the methods used in this study survey to collect data. The questionnaire was used as the instrument for collecting the primary data complemented by interviews, focus groups discussions and documents inspection (Cohen, 2013), while SEM was used to analyse the relationship between insurance fraud, organised crime syndicates and low-income earners. The synthesis of the data collected was presented using various tools on Microsoft Office Word and Excel 2007. Furthermore, it also unpacked and confirmed the perception that insurance fraud compromises national security hence the need to engage the national security intelligence to counter the increasing threat of micro insurance fraud. This chapter sought to analyse and bring out a meaning from the data collected. The analysis component is made up of two sub-components, namely the descriptive analysis using SEM and the confirmatory factor analysis (CFA) analysis.

5.2 Presentation of Results

Presentation of results to this study summarise the main elements of analysed data. Visual presentations, pie charts, and graphics analysis were used to provide summaries of the sample and the metrics. The findings of the study are presented, analysed and discussed in various subsections according to the order in which they appear in the questionnaire. Where

percentages are reported, the figures have been simplified and rounded off to the nearest whole number for ease of interpretation.

5.2.1 Area Coverage

The study focused on Zimbabwe as a whole with an objective to gather data across the country. This was prompted by the fact that targeted insurance companies had decentralised their business from the usual headquarters to provinces and districts. To do so, the researcher divided the target locations into provinces namely Bulawayo, Harare, Manicaland, Mashonaland Central, Mashonaland East, Mashonaland West, Masvingo, Matabeleland North, Matabeleland South, and Midlands as according to Figure 5.1 below. The data for the study came mostly from insurance companies that cover or have branches in the ten provinces. The Zimbabwe Republic Police, the Central Intelligence Organisation, and the Zimbabwe National Army all have permanent posts in the provinces, hence their inclusion in this research. In addition, seventy policyholders from various micro insurance firms from across the provinces were selected.



Figure 5.1. Provinces of Zimbabwe

(Source: Zimbabwe Surveyor General: 2020)

5.2.2 Questionnaire Responses

Table 4.1 below depicts that three hundred and twenty-six questionnaires were received by respondents. Initially, the researcher issued out three hundred and fifty-four questionnaires, however, twelve incompletely filled questionnaires were returned and sixteen questionnaires were not returned all out of the three hundred and fifty-four respondents. This translates to three hundred and twenty-six (326) or ninety-two (92%) of questionnaires to have been returned meeting the required standard of the study while three per cent (3.6%) of the questionnaires returned were incompletely filled and four point four per cent (4.4%) were never returned. The response was an indication that the researcher was able to contact a research population under study that is a representative of the population and industry under study. Response rate of ninety-two (92%) of a targeted total sample size can be generalised to represent opinions of the total population (Cooper & Schindler, 2013).

Table 5.1: Survey Questionnaire Breakdown

INSURANCE INDUSTRY			
NO	INDUSTRY	NUMBER OF PLAYERS	SAMPLE SIZE PARTICIPANTS
1	Short Term Insurance	401	50
2	Life Assurance	415	50
3	Life Reassurance	222	25
4	Micro Insurance	316	35
5	Funeral Assurance	180	20
6	Insurance Brokers	120	10
7	Reinsurance Brokers	26	3
8	Loss Assessors	20	2
	SUB TOTAL	1700	195
9	Policyholders	70	46
	SUB TOTAL	70	46
INTELLIGENCE AND SECURITY SERVICES			
NO	INDUSTRY	NUMBER OF PLAYERS	SAMPLE SIZE

1	President's Department	1	25
2	Zimbabwe National Army Military Intelligence	1	25
3	Zimbabwe Republic Police, Internal Security Intelligence	1	25
REGULATORY AUTHORITY			
1	Insurance and Pension Commission Zimbabwe	1	10
	SUB TOTAL	4	85
	NET TOTAL	1 774	326

(Sources: Owners Compilation)

5.2.3 Industry Coverage

The study stretched across two industries or sectors, namely the insurance industry and the security sector. One thousand seven hundred insurance companies were targeted, one regulatory authority, that is, the Insurance and Pension Commission (IPEC). Two hundred and twelve (212) of the respondents were from the short-term insurance companies, life assurance had fifty (50), life reinsurance had fifty-three (53), micro insurance, twenty-eight (28), funeral assurance, thirty-nine (39), insurance brokers, twenty-two (22), reinsurance brokers, fifteen (15), loss assessors three (3) and sixty-five (65) micro insurance policyholders. Participants from the security sector also contributed to the study with the President's Department had, the Zimbabwe National Army, and the Zimbabwe Republic Police all having twenty-five (25) participants each totalling seventy-five (75) participants. The Insurance and Pension Commission contributed ten (10) participants. Figure 5.2 below exhibiting the participant percentage contribution of the industry under study.

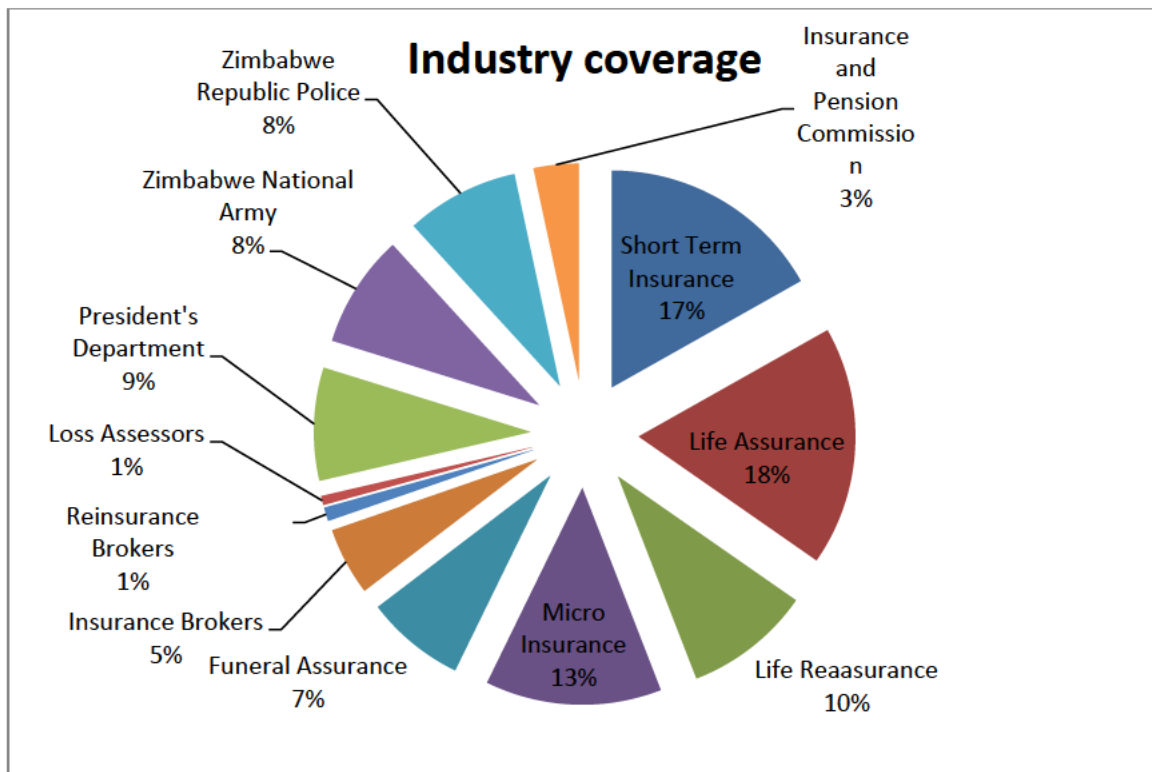


Figure 5.2: Industry coverage

(Source: Owner Compilation)

This study targeted respondents who are working either in the insurance claims and underwriting department and or insurance risk department. In the security sector, the research targeted officers in the anti-corruption units. In that regard, from the three hundred and sixty-two (326) respondents, seventy-five were intelligence officers from the three security intelligence departments, ten from the regulatory authority, seventy policyholders who are also victims of insurance fraud. The researcher noted that job titles varies from company to company, but this study targeted clerks, supervisors, middle managers and department managers particularly those with plus five years' work experience in the insurance industry underwriting department and or insurance risk department. Justification for targeting the above departments is that they are heavily involved in processing insurance claims while the risk department and the security sectors are more into detecting, investigating and minimisation of insurance fraud. However, insurance claims and underwriting department is a target for insurance fraud and, unlike other departments, the insurance claims and underwriting department often encounter insurance fraud (Yusuf & Babalola, 2009). The Insurance and Pension Commission is a governmental organisation that regulates the

insurance and pensions industry in Zimbabwe. It was established under the Insurance and Pensions Commission Act.

5.2.4 Socio-Demographics

Socio-demographics constitute the characteristics of research participant in terms of gender, age, race, and marital status, education and access to micro insurance. Results to this effect were derived from an analysis of the precise three hundred and twenty-six research participants. Figure 5.3 illustrates the gender and race distribution of participants in the study, of the three hundred and twenty-six respondents. Male participants feature prominently at seventy-six per cent and twenty-four per cent female representations. The slightly below average participation of women in the insurance industry, in security intelligence and micro insurance consumption is attributed to the previous historical marginalisation of women both in education, employment and decision making at home. In that regard, the industry is highly dominated by males, but in increase in the participation of women is however, noted.

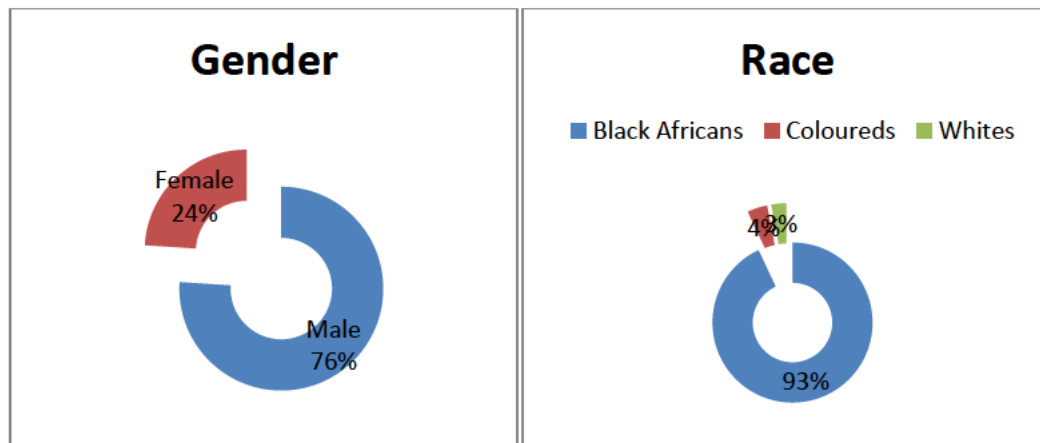


Figure 5.3: Gender and Race

(Source: Owner Compilation)

5.4 Factors Enhancing Insurance Fraud

Factors contributing to insurance fraud in Zimbabwe were obtained from four sources, namely the Insurance and Pension Commission, the Zimbabwe Republic Police Criminal Investigation Department, the Intelligence Community which comprises the President's Department, Police Internal Security Intelligence and the Zimbabwe National Army Military Intelligence Department and various insurance companies. Data collected from the above

organisations and security departments was collaborated and verified with the inspection of documents mainly comprising police criminal dockets and intelligence collected from 2000 to 2021. From the data, factors contributing to insurance fraud in Zimbabwe were grouped into two categories, external and external factors. Externally, this study identified seven factors that contribute to insurance fraud, namely an initiator, perceived reward, and existence of an opportunity, conspiracy, and access to the systems of the targeted insurance company, safety and justification. The factors were ranked on a Likert scale for participants to express their opinions. Figure 5.2 variables organised crime syndicates consider important before considering or commencing a criminal act. The eight identified factors work as an integrated front and the absence of one factor may negatively affect the decision of the whole criminal act irrespective of the type of insurance fraud. The majority of the respondents confirmed that the eight factors are almost equally important. However, inequitable remuneration and preserved reward were ranked the most important factors. These were then followed by opportunity, conspiracy, access, safety and justification, respectively.

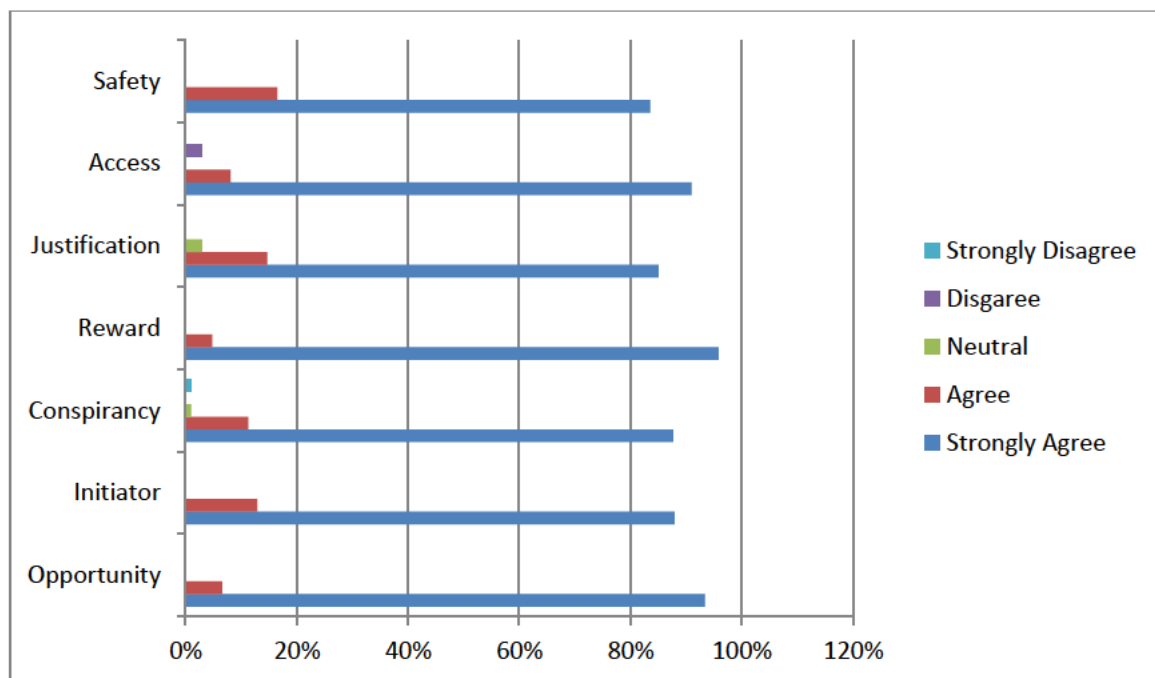


Figure 5.4: Respondents rate on external factors

(Source: Owner Compilation)

An opportunity should also exist. Opportunity refers to circumstances within an insurance company that allows insurance fraud to occur. There are various opportunity factors that can be exploited by organised crime syndicates which may vary from policies, governmental, economic, legislation, law enforcement and social and technological changes (Albanese, 2003). Opportunities internal to the organisation included internal weak controls. These are issues to do with the code of conduct, technology to detect insurance fraud, operational procedures to accounting policies and systems. Internal systems create an opportunity for organised crime syndicates, but are fairly easy to control through organisational or procedural changes (Association of Government Accountants, 2021). Insurance companies offering services to low-income earners hardly invested in fraud countermeasures despite them having a huge monthly income from a huge client base (Insurance and Pension Commission, 2018). Clarke (1997) defines opportunity as the ability to conduct deception. The lack of company control allows fraudsters to conduct a crime. Most encounters with an insurer involve an opportunity, which is frequently a brief circumstance with a perceived low risk but great financial return. According to crime opportunity theory, criminals make logical decisions and hence select targets that provide a large return with little work and danger. The presence of at least one motivated criminal who is ready and prepared to participate in a crime, as well as the conditions of the environment in which that offender is placed, i.e. chances for crime, determine the incidence of a crime. All crimes require opportunity, but not all opportunities result in crime. Similarly, a motivated criminal is required but not sufficient for the conduct of a crime. A big portion of this theory focuses on how changes in lifestyle or everyday behaviours impact criminal chances. Because the offender generally has little or no control over the conditions of the environment, and the conditions that permit particular crimes are often rare, unlikely, or preventable (Jeffery, 1977), opportunity becomes the limiting factor that determines the outcome in environments prone to crime. According to the opportunity theory, when offenders desire to commit a crime, they search for an opportunity or a practical target. Crime chances will be limited by introducing crime prevention techniques through environmental design concepts. Marcus Felson and Ronald V. Clarke outline 10 principles of criminal opportunity theory in their 1998 work, *Opportunity Makes the Thief*, which demonstrate how opportunities, or vulnerabilities, are the fundamental cause of crime. The first five principles are that opportunities play a part in every crime, that crime opportunities are extremely specialised, that crime chances are concentrated in time and location, that crime opportunities depend on daily motions, and that one crime creates opportunity for

another. The final five principles are that some products provide more tempting crime opportunities, those social and technological changes create new crime opportunities, that opportunities for crime can be reduced, that reducing opportunities does not usually displace crime, and that focused opportunity reduction can result in wider decreases in crime.

Initiator. An initiator plays a pivotal role in the initiation of a crime. The initiator identified the opportunity and organizes the people required for the smooth implementation of the crime. Lister (2007) corrupt transaction is often enabled by professionals from many fields and the corrupt intermediaries link givers and takers, creating an atmosphere of mutual trust and reciprocity; they attempt to provide a legal appearance to corrupt transactions, producing legally enforceable contracts; and they help to ensure that scapegoats are blamed in case of detection. CID (2020) postulated that as a matter of fact, organised crimes of an economic nature only succeed because of the aid of professionals, referred to this as professional enablers that are organised by the crime initiator. These professionals are under their expertise able to smoothen the process of commission of the crimes. Cases of insurance fraud against micro-insurance service providers revealed that initiators have common traits that are. Deception is making others believe something that is not true. Concealment, preventing actions from being seen or known about. Fabrication, inventing or producing something false. Coercion is influencing, manipulating or bribing another person to act in a desired way and exploitation is using something for a wrongful purpose. The initiator proposes ideas of how criminal conduct is to be done. These ideas could include new approaches, procedures or structures to solve the problems which confront the group in that regard; the initiator has the following role, information seeker, information provider, problem clarifier and consensus tester.

Conspiracy is also a factor which was highly considered by the respondents. This justified that insurance fraud is an organised crime. Conspiracy is when two or more persons agree to commit a crime together and was categorised as a necessary and important component of organised crime. An agreement between at least two people is required for an act of insurance fraud; an agreement with oneself makes the act impossible (The Criminal Procedure and Evidence Act Chapter 9:07, 2016). Furthermore, the agreement should be entered into with the objective of obtaining a pecuniary or other meaningful benefit, whether directly or indirectly (United Nations Office on Drugs and Crime, 2012). Conspiracy created another important component, namely access. One of the members of the organised crime syndicate

should have access by way of either being an employee, agent or policyholder. The syndicate might also have sub access by recruiting or working with individuals within the targeted insurance company. Access, in this case, meant access to operating procedures, financial status of the company, internal systems and the weaknesses of the system that can be manipulated. A conspiracy occurs when two or more people agree to commit an illegal act and take some step toward its completion. Conspiracy is an inchoate crime because it does not require that the illegal act has been completed. Employee collusion even with external stakeholders is a cause of concern for micro insurance service providers. In a recent report, the ACFE (2019) estimated that the median USA firm loses the equivalent of five per cent of their annual revenue to fraud and that about fifty per cent of fraud cases involve collusion schemes. Moreover, the report shows the median loss of collusive fraud is two hundred per cent higher than the median loss of fraud committed by a single person (ACFE, 2018). Similar findings are reported in two KPMG reports surveying fraud cases. The 2013 KPMG report further points out that collusive fraud is on the rise, as the proportion of fraud cases involving collusion rose from 32 per cent in 2007, to 61 per cent in 2011, and 70 per cent in 2013 (KPMG, 2013). Besides fraud, organizations are also likely to suffer from subtler forms of collusive rent extraction. For example, employees can join forces to game budgeting processes, manipulate performance measures, or obstruct information flows or knowledge transfers. Elements of a conspiracy first require a showing that two or more people agreed to commit a crime. This agreement does not have to be formal or in writing. All that is required is that the parties had a mutual understanding to undertake an unlawful plan. Second, all conspirators must have the specific intent to commit the objective of the conspiracy. This means that someone who is entirely unaware that she is participating in a crime cannot be charged with conspiracy. For instance, if two sisters agree to rob a bank and ask their brother to drive them to the bank without informing him of their intent to commit a crime, he cannot be charged with conspiring in the robbery. This specific intent requirement does not require that each individual knows all the details of the crime or all of the members of the conspiracy. As long as an individual understands that the act being planned is a criminal one and proceeds nonetheless, he can be charged with conspiracy.

Organised crime syndicates engage in insurance fraud once they identify that the criminal act has a reward at the end. Decision-making theorists have long argued that people consider potential risks and rewards before engaging in behaviour, including committing crime

(Beccaria, 2008). People weigh the potential pleasure against the pain that may result from various lines of behaviour and select the course of action with the greatest expected utility (Becker, 1968). The FBI, (2018) noted that organised crime syndicates are self-perpetuating groupings of individuals operating locally or transnational with a primary objective to illegally obtain financial gain and or commercial gains, while constantly seeking power and influence to protect their activities through acts of corruption and violence. The reward has to be real or perceived. With insurance fraud, it has to be deceitful with the intention to illegally or unethically gain at the expense of the insurance company or policyholder. Respondents in this study confirmed that financial gain on the part of individuals involved in insurance fraud remains an important motivator. In addition, justification also acts as a motivator. The organised crime syndicates justified their crime on religious, economic or political basis. Hence is that regard before committing insurance fraud targeted at low income earners, the leader of the group had to come up with justification to indoctrinate other members.

Access. Transnational criminal networks can generate huge sums of money, and like any other business, they require access to organization operations systems, employees and the international financial system to conduct their complex and far-reaching operations. Security on most micro-insurance service providers is physical security, rather than tracking and seizing the money being earned by the criminal networks. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's data in some way that involves fraud or deception, typically for economic gain. Access is however, access in insurance fraud is both physical and technological. Organised crime syndicates usually recruit or work with employees who provide relevant information on insurance company operating system, financial position and loopholes to exploit. As technology advances, so too does fraudulent activity, leaving insurers continuously struggling to protect their financial interests. Fraudsters no longer need to operate on a local level but can span across multiple geographical areas without leaving their home. As technology advances, so too does fraudulent activity, leaving insurers continuously struggling to protect their financial interests. Fraudsters no longer need to operate on a local level but can span across multiple geographical areas. Cyber-criminals engage in online insurance fraud by submitting applications with fabricated data or creating multiple accounts to "double dip" on fraudulent claims. These methods can be validated using human reviews, but this strategy leaves insurance companies open to human error and adds unnecessary

overhead to the application process. Fraudsters use identity fraud to create multiple insurances accounts with synthetic information and stolen equipment, allowing them to double-dip an account for financial gains. Another common strategy for cyber-criminals is account takeover. Usually, an account takeover happens from a successful phishing attempt or when a data breach exposes user credentials across multiple platforms. A cyber-criminal uses a real user account to open policies and then uses these policies to make fraudulent claims on stolen products. Some insurance companies do business online, making it even more challenging to detect and stop fraud. Depending solely on human reviewers requires massive manpower, so using the right tools on insurance applications and online forms saves money and staff overhead, and reduces the risk of fraud.

Safety was also a serious contributory factor. Safety referred to the possibility of the criminal act to be detected and compromised before, during or after the act. The desire for safety and security is not only natural, but also instinctive. Protection and survival from chaotic events, social instability, social disturbance, and physical risks in the human environment are addressed by safety requirements or security demands. One of the most well-known theories of motivation is Abraham Maslow's hierarchy of needs. According to Maslow's hierarchy needs, our behaviours are motivated by physiological and psychological demands that grow from basic to sophisticated. Amongst criminals, safety needs are more visible in emergency situations (Maslow, 1943). This conclusion was reached on observation that organised crime syndicates usually carry out a threat assessment to determine the level of safety. Individuals within an organised crime syndicates usually avoided high risk criminal operations particularly were they have recognised that there is monitoring and a high possibility of detection (Criminal Investigation Department, 2020).

However, the above factor was recognised to be external to the insurance company, there were factors also within the insurance companies offering micro insurance. These factors were deficiencies which were exploited by organised crime syndicates. Figure 5.4 below depict that there basically eight (8) factors namely lack of air tight internal policies and procedures, non-deployment of artificial intelligence, prior employment vetting, lack of counter insurance fraud training and development, lack of policy holder awareness, lack of collaboration with security intelligence and inequitable remuneration.

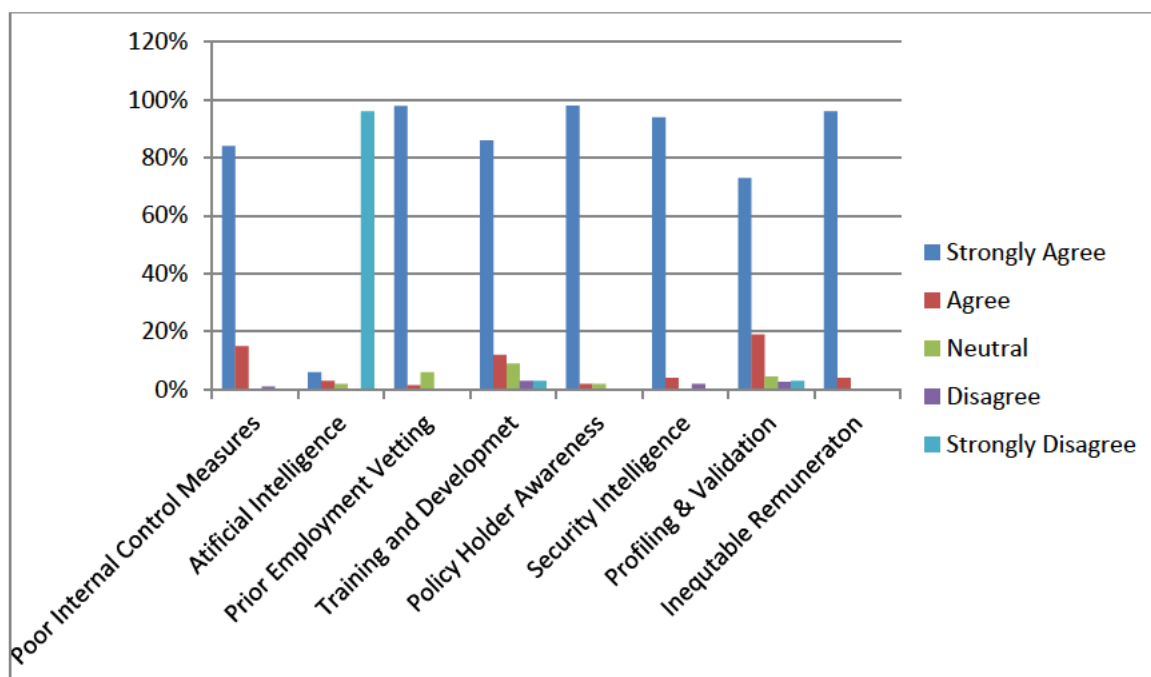


Figure 5.4: Respondents rate on internal factors

(Source: Owner Compilation)

Inequitable remuneration has increasingly become an operational risk in the insurance sector of Zimbabwe. Organisations in the modern world both public and private have since also directed their strategic efforts by focusing on remuneration equity. The 2008 economic crisis in Zimbabwe was characterised by hyperinflation and this compromised remuneration equity (Labour and Economic Development Research Institute of Zimbabwe, 2019). Inequitable remuneration was identified as one of the leading factors that triggered employees in insurance companies to engage in fraud. This was one of the factors that initiated internal fraud perpetrated by employees in micro insurance service providers. Remuneration plays a pivotal role in any organisation to motivate and incentivise performance, loyalty and employee retention (Larkin & Leider, 2012). Poorly remunerated employees in insurance companies are highly likely to engage or easily enticed to commit insurance fraud related crimes (Insurance and Pension Commission, 2018). When it comes to compensation, fair does not always imply equal. According to 2023 Pay Scale study, organisations that utilise performance-based compensation practises may outperform those that stick to equal pay at all costs. Employees understandably detest wage disparities, and an increasing number are asking that action be made to solve the issue. Pay equality concerns have a wide-ranging

impact on the workplace. The first, and arguably most evident, consequence of salary disparity on employee trust and morale (Bartling & vonSiemens, 2011). When the confidence between employee and employer is breached, employees likely to participate in different dishonest, theft-related activities to compensate for low pay or salary. Employees who believe they are being treated unfairly are less likely to perform well and are more inclined to engage in any sort of fraud. Equal pay creates a more content workforce, which may have a substantial influence on productivity. Compensation systems in organisations have a crucial influence in defining employees' attitudes and behaviours; hence, developing fair systems is like pursuing the Holy Grail for human resources practitioners. When it comes to remuneration at work, people conduct assessments to see whether their rewards are equal. Equality theory, established by Adams in the 1960s and 1970s, adequately describes how people determine whether remuneration is fair (or not) and what they behave when they perceive equality (or inequity). Employees analyse whether they are properly paid in exchange for their efforts, and they also engage in social comparisons by evaluating their inputs and returns with those of their colleagues. People's behaviours will alter if they perceive inequitable pay (Baron & Kreps, 2013).

Internal control through the effective and religious implementation of internal policies and procedures remain paramount in countering insurance fraud. A fraud policy and procedure is an important tool for conveying organisation's attitude on fraud and how it will be dealt with. Micro insurance service providers are however, still lagging on this aspect. A fraud policy informs employees what reaction measures have been developed to deal with and mitigate the harm caused by any fraudulent attack. By specifically describing fraudulent conduct, workers and third parties understand what is and is not acceptable. A well drafted fraud policy that is communicated to all employees, contractors and suppliers is an economical way of indicating that the fight against fraud is endorsed and supported at the most senior level, and may lessen the risk of your business becoming a victim. This should however, be complemented by the deployment of artificial intelligence. By monitoring and analysing client behaviour, checking papers, and identifying questionable conduct, artificial intelligence can aid in the prevention of fraud. One significant advantage of AI fraud models is that they improve in accuracy as more data is given into them (Boyer, 2000). The aspect of employee vetting and security clearance is still at its infancy amongst micro insurance service providers. Profiling and validation is a method that is used during the hiring process to identify the right potential

candidates for a particular job profile or position within a company. Usually takes place before hiring; the process needs to be unbiased and unprejudiced. Employee profiling is an effective way for companies to understand their employees' personalities, skills, and traits in an objective manner better. By analysing this information, employers can make unbiased decisions regarding hiring, training, and development opportunities. In recent years, psychometric tests and personality assessments have become popular tools for employee profiling. These tests offer objective data to help businesses identify potential hires and current employees' strengths and weaknesses. However, quite often, profiling is misinterpreted as validation. Validation also involves assessment of an individual's identity, profile and reputation. This is done through verification of employment details, education credentials, criminal records, address and much more. However, verification is different from Profiling. The objective is to deter criminal from being recruited while training and development will equip the individual with prerequisite skills to counter insurance fraud. Micro insurance service providers also need to take a proactive action to counter insurance fraud. Organizations need to be able to go outside the firewall to gather as much threat actor information as possible to build robust internal defences against fraud. It could be argued and rightly so that employees are a company's greatest asset, and, therefore, investing in their training and development is key to sustaining business growth and success. This commitment makes sense when the lengthy processes businesses carry out to recruit and hire qualified staff are considered. Training and development do not lead only to increased sales, but rather to a more enlightened workforce that can deliver the required outcomes.

Security intelligence refers to the practice of collecting, standardising and analysing data that is generated by networks, applications, and other real-time applications, and the use of that information to assess and improve an organization's security posture. The discipline of security intelligence includes the deployment of software assets and personnel to discover actionable and useful insights that drive threat mitigation and risk reduction for the organization. Insurance fraud has risen dramatically and the trend looks likely to continue due to the effects of financial stress and increased living costs, driven by the economic climate in Zimbabwe. On the flip, insurers are committed to protecting honest policyholders from the cost of insurance fraud, whilst providing policyholders with the highest levels of claims service. Effective investigation is an essential part of the claims process, allowing insurers to detect and manage fraud, save money and reduce the cost of premiums. Insurers

face an ever-increasing requirement to provide excellent customer service, manage total claim costs, reduce the lifecycle of claims and meet claimants' legitimate expectations. Speed is of the essence so that honest policyholders have a positive customer experience and are reinstated swiftly. However, whilst claims must be validated quickly, it is also essential that the validation process is undertaken properly, to ensure that the premium pool, which is funded by all policyholders, is not depleted by fraudulent activities. Effective investigation and the delivery of excellent customer service need not be mutually exclusive. Insurers can use technology and counter-fraud intelligence services to speed up investigations, delivering operational efficiencies and reducing the time taken to collect and integrate key information. Investigation management systems can assist insurers with mitigating risk and optimising their counter-fraud resources most effectively. Tools can complement existing anti-fraud strategies and now provide insurers with a single point of access, in real-time, to extensive consumer intelligence. Systems and workflow processes can be streamlined to create an immediate profile of a customer, together with their claims history and provide insurers with a consolidated view of the risk and potential areas requiring further investigation. Certainly, the market as a whole recognises the potential reputational risk linked to claims fraud investigation. The insurance market recognises that increased cooperation, joined-up thinking and a collaborative approach to the management of fraud are vital to staying one step ahead of the fraudsters. Insurers promote their position on fraud to varying degrees. A 'zero tolerance to fraud' reinforced at the individual insurer level would act as a strong deterrent to 'would-be' opportunists and organised fraudsters.

5.5 Analysis of Behavioural Responses

This section offers an analysis of responses from the five-point Likert scale section of the questionnaire. To assess attitudes, knowledge, perceptions, values, and behavioural changes, a Likert scale was deployed. A Likert-type scale consisted of a set of statements from which respondents selected, to rate their responses to evaluative questions (Vogt, 1999). To ensure reliability and validity, the likert scales should be tested not just for internal consistency, but also for unidimensionality (Schrum et al., 2020:8). As a result, unidimensionality is the belief that measuring items or indicators belonging to the same scale convey differences in the same underlying entity (Ziegler & Hagemann, 2015:231). Table 5.2 below, typically, exploratory factor analysis was performed to determine if a set of items measure the same thing. As a result, the latent component loadings are shown with the aggregate response to each indicator

for all items on the scale that measures the relevant construct. Higher values for this factor indicated that the item accurately assesses the construct it is supposed to test. Scale items are frequently derived from the specification of the construct being measured. This approach of creating measuring items is intended to verify that all items accurately represent the construct. As a consequence, measurement items or indicators belonging together in a scale are believed to capture differences in the same underlying construct; this is unidimensionality (Ziegler & Hagemann, 2015:231). Exploratory factor analysis was typically used to test whether or not a set of items measure the same attribute. For this reason, the latent factor loadings are presented for all the items on the scale that measures the relevant construct alongside the aggregate response to each indicator. Higher values of this factor would depict that the item satisfactorily measures the construct it intends to measure.

Table 5.2: Likert Scales Responses

	Do criminals in insurance fraud capitalise on existing opportunities to commit their crimes.	Is a crime initiator an important component in initiating insurance fraud?	Does the crime need to be organised between two or more people.	Are criminals motivated by the end reward to commit insurance fraud?	Do criminals require any form of access to the internal system of the insurance company to successfully complete their criminal act.	Is safety an important factor in insurance fraud crime?	Does improvement on employee remuneration a possible insurance fraud counter measure?	Can artificial intelligence reduce or counter insurance fraud.	Is employee security prior employment vetting a proactive counter measure?	Are internal control systems an effective counter measure?	Is policy holder and public awareness a measure that can reduce insurance fraud	Can policy holder security clearance through profiling and validation aid in reducing insurance fraud.	Is intelligence sharing between insurance companies and national security intelligence a recommendable counter measure?
Valid	326	326	326	326	326	326	326	326	326	326	326	326	326
Missing	0	0	0	0	0	0	0	0	0	0	0	0	0
Strongly Agree	97.50%	97.50%	92.90%	100%	90.50%	90.80%	80.10%	92%	96%	85.90%	78.80%	78.80%	89.30%
Agree	2.50%	2.50%	4.30%	0	9.50%	8.60%	12.60%	8%	4%	14.10%	15.60%	16.30%	9.50%
Neutral	0	0	1.20%	0	0	0.60%	0	0	0	0	0	1.20%	1.20%
Disagree	0	0	1.50%	0	0	0	2.10%	0	0	0	3.70%	2.50%	0
Strongly Disagree	0	0	0	0	0	0	5.20%	0	0	0	1.80%	1.20%	0

(Sources: Owners Compilation)

5.6 Confirmatory Factor Analysis

Confirmatory factor analysis is a Structural Equation Modeling (SEM) and factor analysis method which was used in this study to determine if observed variables contribute to latent or unobserved variables. The factor structure of a collection of observed variables was statistically verified using CFA. The researcher deployed the Confirmatory Factor Analysis (CFA) to assess whether there was a link between observable variables and their underlying

latent components (International Encyclopaedia of the Social and Behavioural Science, 2001). In Confirmatory factor analysis, SEM, the researcher hypothesised a set of relations that existed among a set of variables, based on a theoretical framework (Crano, Brewer & Lac, 2015:173). Structural Equation Modeling (SEM) is the preferred statistical analysis to addressing the primary research objective of developing a conceptual framework of factors that enhances or influence be it an individual or a group of people to commit insurance fraud. Structural Equation Modeling (SEM) involves the construction of two models, the measurement model specifying the relationship between latent variables and their respective indicators or measuring items and the structural model specifying inter-relations of latent variables in the analysis. The first step in SEM is to specify the measurement model and conduct Confirmatory Factor Analysis (CFA) to test for unidimensionality, validity and reliability of items measuring the latent variables or constructs (Awang, Afthanorhan, Mamat & Aimran, 2017).

One latent construct, insurance fraud was the measurement model. Insurance fraud was measured directly by multiple questions. Hence in that regard, the CFA approach computes the factor loading for each item measuring latent constructs (Awang et al., 2017). Error terms are modelled for each item when computing the factor loading. This allows for the elimination of items with large measurement error and/or low factor loadings, thus improving the quality of the latent construct modelled (Hair, Gabriel & Patel, 2014). Using the CFA method, the model was then examined for any potential problematic estimates, specifically those with low factor loadings. The regression weights (factor loadings) for the common factor and each of the indicators are shown in the pathways diagram below Figure 5.6. The squared multiple correlation coefficients (R^2) are also shown, which describe how much variance the common factor accounts for in the observed variables.

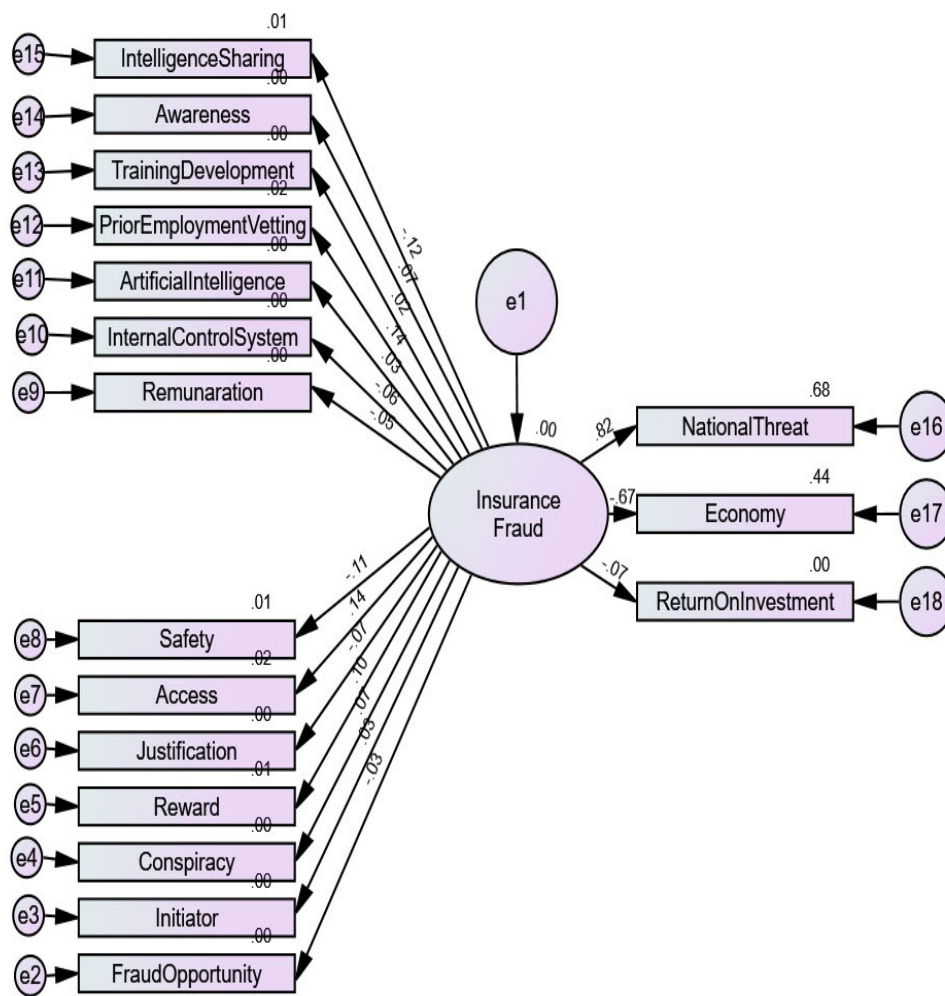


Figure 5.5: Structural model with unstandardized regression weights

(Source: Structural Equation Modelling)

As exhibited in Figure 5.5 above, the unstandardised beta estimate for the effect of internal and external causes to insurance fraud also with the threat of insurance fraud. External causes, one out of the seven factors, safety has a negative influence on fraud while other factors namely access, justification, reward, conspiracy, initiator and opportunity have a statistically significant positive influence on insurance fraud. The positive sign though implies that an increase in one factor has a positive impact on insurance fraud while a negative impact on external variables has also a negative impact on insurance fraud. This is however, unlike the internal causes of insurance fraud. Three variables namely intelligence sharing, remuneration and internal control systems have negative factor loadings implying

that a reduction in these variables impacts or enhances insurance fraud while the other variables training and development, security intelligence sharing and prior employment vetting all impact positively on countering insurance fraud. Unstandardized regression weights are derived from the covariance matrices or the raw data. Unstandardized comparisons are desirable when comparing between groups (across samples) and the groups have differing variances. There were two types of variables namely observable or manifest (endogenous or dependent) variables and latent (exogenous or non-observable) variables in the hypothetical model. Observable variables are indicators of the underlying construct represented by the observable variables, whereas latent variables are theoretical structures that cannot be directly observed. In that regard, confirmatory factor analysis was done to test a factor structure's hypotheses. Each arrow from a latent variable F1 (insurance fraud) to a variable is a value that can vary from -1.0 to 1.0, with higher numbers (positive or negative) indicating a stronger link (Figure 5.5). The indicator weights of factor loadings are unstandardised to values between -1.0 to 1.0. Weight close to 0 indicated a weak relationship of the factor loading with the construct, whereas weights close to +1 (or -1) indicated a strong positive (or negative) factor loading (Sarstedt & Ringle, 2019). Figure 5.5, factors enhancing insurance fraud were categorised as follows. External factors factors, opportunity, initiator, conspiracy, reward, justification, access and safety. Of these seven factors three namely opportunity (-.042), justification (-.109) and safety (-.184) have negative factor loadings, which means that reducing any of these factors reduces the chances of insurance fraud. The other factors with positive factor loadings namely initiator, conspiracy, reward and access are actually enhancers of insurance fraud, their increase has a positive impact or increases the chances of insurance fraud. On internal factors, However, this excludes remuneration, remuneration has a positive factor loading of 1.00, this implies that an increase in remuneration amongst employees have a possibility to reduce insurance fraud while the reduction increases insurance fraud. On the external factors which include remuneration, internal control systems, artificial intelligence, training and development, awareness and intelligence sharing. In the category of internal factors only three namely remuneration (-.086), internal control systems and intelligence sharing have negative factor loading. Their reduction in any form increases chances of insurance fraud.

Unstandardized beta estimates provide for an understanding of relationships expressed in terms of standard deviations (Grace & Bollen, 2005:290). In these variables, it was observed

that if any or either of the internal or external variables were increased by one standard deviation, insurance fraud would be expected to increase. In that regard, hypothesis tests present a simplified model of the real world that can either be ‘confirmed’ or ‘ejected’ through analysis and summarisation of data relevant to the underlying theory (Westland, 2015:145). Results of the study hypotheses testing based on the structural model show that study research questions are answered and the variables identified in relation to the research questions have a large positive effect on insurance fraud.

Table 5.5: Regression Weights

NationalThreat	<---	Insurance_Fraud	1.000
Economy	<---	Insurance_Fraud	-.899
ReturnOnInvestment	<---	Insurance_Fraud	-.277
FraudOpportunity	<---	Insurance_Fraud	-.041
Initiator	<---	Insurance_Fraud	.034
Conspiracy	<---	Insurance_Fraud	.102
Reward	<---	Insurance_Fraud	.160
Justification	<---	Insurance_Fraud	-.109
Access	<---	Insurance_Fraud	.235
Safety	<---	Insurance_Fraud	-.184
Remuneration	<---	Insurance_Fraud	-.086
InternalControlSystem	<---	Insurance_Fraud	-.043
ArtificialIntelligence	<---	Insurance_Fraud	.021
PriorEmploymentVetting	<---	Insurance_Fraud	.198
TrainingDevelopment	<---	Insurance_Fraud	.030
Awareness	<---	Insurance_Fraud	.102
IntelligenceSharing	<---	Insurance_Fraud	-.169

(Sources: Owners Compilation)

Table 5.5 above and Table 5.6 below give explicit regression weights, the categorisation of unstandardized regression weight based on their values is a proposed reasonable method to describe a causal effect or magnitude of an association (Essentials of Structural Equation Modelling, 2018). Unstandardized regression weights in the analysis emanated from regression analysis estimates where all data was standardised so that the variances of variables, both independent and dependent, were equal to one (1). The figures depict that the unstandardised regression weights are unit-less and refer to how many standard deviations increase in the predictor variable. The first three items depict the types of threats posed by insurance fraud. The conclusion is that insurance fraud has negative impact to the economy and return on investment figures with a negative value -.277 and -.899 respectively depicts

that when insurance fraud goes up, the economy and return on investment goes down by the stated values. Ironically, national threat has a positive value of 1.000 which is a conclusion that insurance fraud is a threat to national security. When insurance fraud increases, national security is also compromised with a value of 1.000.

With regards to external factors, opportunity (-.041), justification (-.109) and safety (-.184) which all have negative values can to be interpreted in the same way with with internal causes of insurance fraud intelligence shareing (-.169), internal control systems (-.043) and remuneration (-.086). This implies that the reduction of these internal and external factors enhances insurance fraud.

5.7 Total effects

The entire effect of endogenous variables on exogenous variables is commonly expressed as the fundamental bivariate association of exogenous variable (Insurance Fraud) with endogenous variables (Azman, 2017). Table 5.6 depicts the primary paths via which endogenous variables might influence the exogenous variable directly or indirectly. The total effect (combined direct and indirect effect) of each column variable on each row variable. Direct effects are by definition "direct" effects, which are basically the direct loading of variables to another while indirect effects are effect on variables on other variables when there are direct paths between them. Table 5.6 depicts that endogenous variables have a direct effect to the exogenous variable (Insurance Fraud). This concludes that a direct relationship between the two variables exists with variables with positive factor loadings while those with negative factor loadings have a negative impact on the exogenous variables. The causal effect is that an increase of any of the endogenous variables increases the chance of insurance fraud. Also, to note is that, while direct effect has a positive causal effect, endogenous variables indirect effects have values at .000. This implies that endogenous variables have no indirect causal effect to the exogenous variable.

Table 5.6: Total Effects

	Insurance_Fraud
ReturnOnInvestment	-.277
Economy	-.899
NationalThreat	1.000
IntelligenceSharing	-.169
Awareness	.102
TrainingDevelopment	.030
PriorEmploymentVetting	.198
ArtificialIntelligence	.021
InternalControlSystem	-.043
Remuneration	-.086
Safety	-.184
Access	.235
Justification	-.109
Reward	.160
Conspiracy	.102
Initiator	.034
FraudOpportunity	-.041

(Sources: Owners Compilation)

The sum of all direct and indirect impacts is the total effect, because the individual standardised path coefficients may likewise be > 1 , the standardized overall effect may already be > 1 , for example, due to collinearity or a suppression effect. Partial regression coefficients are path coefficients. The relationship exhibits that variable with a positive attribute an increase in reward amongst employee reduces the possibility or threat of internal insurance fraud while variable with negative attributes such as Criminal vetting, technology, internal controls and intelligence sharing have negative impact on insurance fraud. Conclusively, the model exhibits an important relationship between insurance fraud and internal and external factors. To note is that internal and external causes of insurance fraud are interdependent.

5.9 Model fit

Various goodness-of-fit indices are proposed in the literature to assess model adequacy, which addresses construct validity. Commonly reported goodness of fit indices included the Comparative Fit Index (CFI), Tucker-Lewis Index (TLI), Goodness-of-fit Index (GFI) and the Root Mean Square Error of Approximation (RMSEA). As a rule of thumb if CFI and TLI are greater than 0.90, the model is deemed acceptable, while a value greater than 0.95 indicates good fit (Hox & Bechger, 1998). The analysis reached the minimum requirement in

terms of the sample size of three hundred and sixty (362) participants, a Chi-square of 43.576, probability level of .023 and a degree of freedom of .27. The hypothesis-driven approach is a defining feature of CFA (Brown, 2015). The researcher came up with a theory on the model structure, which he expressed as specific factor (s) underlying a group of elements. The value 43.576 is the approximate probability of generating a chi-square statistic as large as the chi-square statistic obtained from the present set of data if the required distributional assumptions are met and the provided model is true. For example, if the probability level is .05 or less, the data deviates significantly from the model. In this scenario, a model in the structural equation model with zero degrees of freedom is referred to as a saturated model. The data is perfectly fit by the saturated model. The model cannot be defined if the degree of freedom is negative. If the degree of freedom is not negative, that is, zero or positive, the model can be defined.

Table 5.6: The Model

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	50	413.492	120	.000	3.946
Saturated model	170	.000	0		
Independence model	17	484.552	153	.000	3.167

(Source: Structural Equation Model)

NPAR is the number of distinct parameters (q) being estimated in a study. Models with relatively few parameters (and relatively many degrees of freedom) are sometimes said to be high in parsimony, or simplicity while models with many parameters (and few degrees of freedom) are said to be complex, or lacking in parsimony. While one can inquire into the grounds for preferring simple, parsimonious models (e.g., Mulaik, et al., 1989), there does not appear to be any disagreement that parsimonious models are preferable to complex ones. When it comes to parameters, all other things being equal, less is more. At the same time, well-fitting models are preferable to poorly fitting ones. Many fit measures represent an attempt to balance these two conflicting objectives, simplicity and goodness of fit. In this model fifty (50) parameters to be estimated is deemed to be average. However, CMIN is the minimum value of the discrepancy while DF is the number of degrees of freedom for testing the model ($df = d - p - a$). $CMIN/DF$ is the minimum discrepancy, C divided by its degrees of freedom. C/d .

CMIN 413.492

DR	120.00
=	3

Several scholars in SEM have suggested the use of this ratio as a measure of fit, the ratio should be close to one for correct models. However, there is no clarity on how far from one should let the ratio get before concluding that a model is unsatisfactory. Wheaton et al. (1977) recommended that the researcher should compute a relative chi-square X^2/df hence suggested a ratio of approximately (5) five or less as beginning to be reasonable and the range of two (2) to one (1) or three (3) to one (1) are indicative of an acceptable fit between the hypothetical model and the sample data." (Carmines & McIver, 1981). Different researchers have recommended using ratios as low as 2 or as high as 5 to indicate a reasonable fit." (Marsh & Hocevar, 1985). The hypothesised factor structure is then used to determine how much of the covariance between the items may be recorded (Hooper, Coughlan & Mullen, 2008). Evaluation of the proposed model's goodness of fit, which represents how well the model matches the observed data, is an important stage in CFA, in addition to examining the covariance reflected by the model (Hooper et al., 2008). An effort to examine the measurement model dependability was done using the Cronbach's alpha and composite reliability. Cronbach's alpha is reactive to the number of items and, in general, overestimates internal consistency dependability. Different indices of dependability are evaluated when Cronbach's alpha is combined with composite reliability, which eliminates the underestimation associated with Cronbach's alpha (Hair et al., 2014). If the Cronbach's alpha is more than zero point seven (0.7) for all constructs, showing acceptable internal consistency. Above zero point six (0.6) composite reliability suggests latent variable reliability and internal consistency as a measure of internal consistency (Awang, 2012).

5.9.1 Cronbach Alpha

A poorly formed scale may result in data that does not assess the intended study hypothesis. Thus, before any inferential statistical tests are applied to a Likert scale, it is best practice to test the quality and reliability of scales adopted for research (Schrum et al., 2020). Scale reliability was assessed using Cronbach alpha and tested the four constructs. The common rule of thumb is that a scale with a value of Cronbach's alpha above 0.7 demonstrates acceptable internal consistency, though the closer to 1.0 this value is, the better. Cronbach's

alpha below 0.7 is cause for concern, indicating that at least one of the items is adversely affecting the scale's reliability (Hinton & Platt, 2019).

Table 5.7: Scale reliability and validity statistics

Research Objective	No. of Items	Mean	Cronbach's Alpha Coefficient
Investigate the causes of insurance fraud in the microinsurance industry in Zimbabwe	30	2.42	0.18
Evaluate the impact or threat level of insurance fraud targeted at low-income earners to national security and interest	20	3.01	0.84
Assess the role of security intelligence organisations in countering insurance fraud in the microinsurance sector in Zimbabwe	30	2.42	0.18
Prescribe other strategies that can be fused with security intelligence to counter insurance fraud in the microinsurance sector in Zimbabwe	19	2.10	0.74
Overall Cronbach Alpha	119	2.78	0.8

The four constructs calculated 2.24, 3.02, 2.42 and 2.10. The aggregate alpha yielded a result of 0.8. This result indicates that the scales are reliable according to the measurement criteria, reporting satisfactory coefficient alpha values.

5.10 Chapter Summary

The insurance industry has over years positioned itself to be an important component of human security in Zimbabwe. Services in the insurance industry are constantly stretching to low-income earners which include civil servants, farm workers, mine workers, house maids, drivers, and casual workers in various industries, amongst others. The enormous numbers of low-income earners have made this market segment attractive to insurance companies as well as organised crime syndicates considering that it has high levels of monthly income from subscriptions. Despite the market segment being attractive, insurance companies venturing into this market are reluctant to invest in proactive measures that counter insurance fraud by

organised crime syndicates. A lesson learnt from this study envisions that insurance fraud is increasingly becoming a national security threat since money obtained from the criminal conduct is easily invested into other criminal acts. The government, companies and citizens are most likely to fall victims and the failure by the police to respond to the risk undermines public confidence (KPMG Zimbabwe, 2021). In that regard, Schewed (1993) avers that insurance fraud and fraud in general are highly concealed crimes. In most cases, fraud goes undetected and unpunished as well. This is due to the reactive nature of how the police conduct their business. The police cannot arrest before a crime is committed (Criminal Procedure and Evidence Act, 2009). It is against this background that the security intelligence agencies are mandated to deal with, counter threats to national security and interest; security intelligence can be deployed to counter insurance fraud and contain criminal operations by organised crime syndicates. The proactive nature of intelligence work becomes imperative in this case. Such conclusions were reached based on data analysis, which was proven by the use of an acceptable research technique, design, and statistical tools to support the study objectives. The results of the statistical tests exhibited a hypothesised path relationship between insurance fraud and factors causing insurance fraud which were both statistically significant.

The following chapter, chapter six (6) will explain the study's primary findings in relation to the research objectives.

CHAPTER SIX

DISCUSSION OF FINDINGS

6.1 Introduction

This chapter, examines and discusses the study findings which were influenced by the research objectives outlined in chapter one. The researcher has applied primary and secondary data to answer the research questions while in sync with the research objectives through the application of research techniques as prescribed in Chapter four (4). The study's overall goal was to look into the reasons of insurance fraud in insurance businesses that provide services to low-income earners in Zimbabwe. Furthermore, it sought to identify the sources, effects and threats of insurance fraud. Insurance fraud is regarded as a threat to national security and interest, hence, the study was aimed at dissecting the practicality of the national security intelligence organisation as a possible countermeasure to complement already existing strategies to counter insurance fraud. In that regard, chapter six (6) begins with a summary of the demographic profile of low income earners in Zimbabwe, thereafter the empirical findings of the study are supported by literature review and official publication reports by responsible authorities in effort to bridge or narrow the knowledge gap between academic and practitioners' standpoints. Further to the demographic characteristics of research participants, this chapter goes further to dissect on the causes of insurance fraud in the low income sector of Zimbabwe.

6.2 Profile of Low Income Earners

Zimbabwe had a population of fifteen million one hundred and seventy-eight thousand people as of April 20, 2022, with seven million two hundred and eighty-nine thousand five hundred and fifty-eight, forty-eight per cent male and seven million eight hundred and eighty-nine point four hundred and twenty-one, fifty-two per cent female, for a sex ratio of ninety-two males to every one hundred females (Zimbabwe Census Report, 2022). In 2019, forty-two per cent which increased to sixty-one per cent of the total Zimbabwean population lived in extreme poverty, below the international poverty line of USA one dollar ninety per person per day. Summaries of the research participant indicated that there is an appetite for micro-insurance services amongst low-income earners in Zimbabwe. Study demographics pointed out that the majority of research participants, policyholders qualified to be in the category of low-income earners, black African males living in a household of between four and six

people all being sustained on a daily income of between USA two and ten dollars. Monthly, low-income earners earn an average of between one hundred and one hundred and fifty USA dollars and this covers both food and non-food requirement including servicing of monthly insurance premiums. A significant percentage of the population in Zimbabwe is in extreme poverty and falls under the category of a low income earner. The situation was exacerbated by the combined effects of rising food prices, economic contraction induced by the COVID-19 epidemic, and poor harvests (Rapid Poverty Income Consumption and Expenditure Survey (PICES) 2020). A telephonic survey done by the Zimbabwe National Statistics Agency (ZIMSTAT) in collaboration with the World Bank and UNICEF to measure the socio-economic impact of COVID-19 on households in Zimbabwe revealed that the coronavirus pandemic's socio-economic effects continue to cause suffering in communities with low levels of income and food insecurity level remained high, affecting seventy per cent of the total population. In most parts of Zimbabwe, insurance is rather viewed as an unnecessary expense and only for the rich, that belief has been passed from generation to generation hence becoming a culture. The findings of this study confirmed the prior expectation, the expectation that insurance culture has a significant, direct effect on the uptake of insurance services by low-income earners. According to various sources of literature, culture plays an influential role in influencing low-income earners' participation in insurance markets and uptake as well (Zhong et al., 2015:41); therefore, the implications of culture, norms, and values should be understood before venturing into a market because cultural differences produce different insurance participation outcomes. The context is that consumers differ and hence respond differently to insurance solicitations, particularly in terms of cultural beliefs rather than economic logic (Park & Lemaire, 2012). Insurance fraud threats and state of countermeasures

Over the years, organised crime has become one of the most powerful economic and militaristic forces in the world. The threat posed by organized crime to world peace, progress, and even national sovereignty has increased. In addition to using guns and brutality, the criminals engaged collect the money necessary to support their actions through various forms of fraud, such as insurance fraud. They also use money and bribery to buy elections, politicians, and positions of authority, including the military. Figure 6.1 below shows that amongst the three hundred and thirty three participant, eighty-three point two participants alluded the the nortion that insurance fraud was a fraud to national security and interest.

Table 6.1: Frequencies: Insurance fraud a threat to national security and interest.

Does insurance fraud affect operations, viability and rreturn on investment of insurance companies			Is insurance fraud a threat to national economic development?			Is insurance fraud a threat to national security?		
	N	%		N	%		N	%
			Disagree	6	1.8%	Disagree	3	0.9%
Neutral	2	0.6%	Neutral	23	7.1%	Nuetral	15	4.6%
Agree	52	16.0%	Agree	140	42.9%	Agree	139	42.6%
Strongly Agree	271	83.1%	Strongly Agree	157	48.2%	Strongly Agree	169	51.8%

An inspection of classified intelligence and organised crime cases in the microinsurance sector revealed that organised criminal syndicates in Zimbabwe pose a threat to economic development and operations, subsequently return on investment to micro insurance service providers because of how they have quickly targeted, infiltrated, and adapt in the insurance sector. They are also a formidable force to contend with, so pervasive that they posed a danger to national security. A profile of three hundred and twenty-one organised crime groups operating only in Zimbabwe, one hundred forty-two target micro-insurance service providers (Security Intelligence on Organised Crime, 2020). Further, the study unveiled that, due to regional contagion, the problem of insurance fraud is no longer limited to Zimbabwe, but the same organised crime groups have linked with regional organised crime groups and all targeting micro-insurance service providers (Oaks, 2021). This study has acknowledged that there are various factors which organised groups exploit to be successful in their criminal operations, factors such as the increasing power of technology, the global influence of terrorist groups and the global economic downturn is creating justifications to commit insurance fraud. Organised crime syndicates operate globally, conducting various criminal activities including fraud, drugs, arms and human trafficking, cybercrime and terrorism. Billions of dollars of money obtained via insurance fraud are wired across the world annually, distorting economies, corrupting government officials, law enforcement agents and vital government institutions and as well as fuelling civil conflict. Globally, organised crime has become a major issue on security intelligence briefs and security affairs, a crucial factor with a direct impact on international economy, security and an immediate reality for governments, legislators, intelligence personnel, law enforcement agents and general public

globally. Aside from the direct effects of financing terrorism and insurgency, drug, human and arms trafficking, cybercrimes, environmental damage and various organised crime activities that can undermine the rule of law and good governance, without which there can be no sustainable development (United Nations, 2019)

According to our data, fraud attempts are becoming more varied and diversified and included anything ranging from account takeovers and personalised phishing scams to identity theft. Microinsurance service providers, therefore, require multi-layered counter-insurance fraud solutions with advanced identification, authentication, and behavioural biometrics capabilities to combat this vast variety of threats. However, regrettably, this study identified a very low zeal amongst micro-insurance service providers to invest in such technology irrespective of the availability of funds. The situation was worsened with the use of various devices, access channels, and mobile apps by policyholders hence this has made aberrant behaviour no longer a reliable indicator of fraud. Because of this, detecting insurance fraud is more difficult and calls for a more in-depth study of behavioural biometrics data, such as the customer's location, the device they're using, and "out of character" transactions and requests. As security measures advance, organised crime groups have employed the use of computer and software engineers to continuously develop new technology meant to get around them. In reality, organised crime groups are known to make use of technology, frequently acclimating to new developments more quickly than micro-insurance service providers. Some of the more recent scam kinds that are still expanding quickly include man-in-the-middle or man-in-the-browser attacks, when fraudsters use a legitimate customer's gadget to their advantage, getting through device identification and authentication defences. Use of mules, where a person, known as a "mule," knowingly lends their identity to a fraudster to conduct a crime, like signing up for a cell phone contract and later selling the phone and artificial intelligence attack, for instance, "machine-to-machine" fraud, in which artificial intelligence bots interfere with production processes, or to submit a large number of false account applications.

Given the situation above, research findings on insurance fraud in Zimbabwe significantly confirmed that insurance fraud has become a threat to Zimbabwe's national security and a regional and global threat. Inspection of Zimbabwe Republic Police documents since 2000 acknowledged that fraud in general and insurance fraud, in particular, is on a rise, but all cases of fraud are difficult to prove in the courts of law (Zimbabwe Republic Police, 2000). Ninety-one per cent of the respondents strongly agreed that insurance fraud is a threat to

national security and the insurance industry, while nine per cent agreed with the same sentiments. In that regard, the same respondents confirmed that insurance fraud is a covert crime which requires the proactive covert tradecraft deployed by intelligence operatives, rather than the reactive approach by the police. A basic intelligence cycle tool can be deployed by intelligence officers or intelligence organisations to counter insurance fraud-related cases. This is important as it is rather a proactive countermeasure that restricts organised crime syndicates to commit fraud (President's Department, 2019). The British Broadcasting Corporation (2021) has also noted the need for the British intelligence community to play a greater role in countering insurance fraud. Fraud is the most common crime, costing up to one hundred and ninety billion British pounds each year due to the volume of credit card, identity, and cyber-fraud. As a result, intelligence services should be better equipped, resourced, and collaborate more closely with the business sector in this area.

6.3 Findings Related to Types of Insurance Fraud

Findings unearthed that there is rampant insurance fraud in the low-income sector insurance market. According to Patel (2002), the informal sector accounts for between fifty and sixty per cent of the workforce in most less economically developed African countries. It can reach ninety per cent in extreme cases, given that most people in Africa begin working at the age of ten for males and twelve for females. Zimbabwe is included in which serious crimes related to insurance fraud in the low-income earner's market are continuously increasing. The Zimbabwe insurance industry regulatory authority the Insurance and Pension Commission (2019) therefore defined insurance fraud as an act that involves a policyholder or a third party in a claims process, in which either party consciously provides wrong or false information or misrepresents material facts during the claims process to swindle the insurance company of money or any benefits which they are not entitled to. Further, according to Figure 5.4 below, the Insurance and Pension Commission (2019) has identified six most prevalent types of insurance fraud in Zimbabwe and these have been confirmed by ninety-eight per cent of the respondents. In descending order, syndicate fraud also known as organised fraud in the low-income sector constitutes forty per cent of insurance fraud. Australian Organised Fraud and Intelligence Group (2017) defined syndicate fraud as an organised criminal act conducted by syndicates or organised groups that target and penetrate insurance companies and policyholders, most commonly for profit. This is a hybrid type of insurance fraud in which organised crime syndicates, employees and policyholders work together to swindle insurance

companies. Low-income earners who are policyholders, under their compromised income status are easily enticed to engage in this kind of crime. Secondly, thirty-two per cent of the cost of insurance fraud is attributed to opportunistic fraud. Opportunistic fraud was prevalent during the coronavirus-induced restrictions period. It was being conducted on any sort of insurance, from personal injury claims in automotive or commercial liability to property, pet, or travel insurance and beyond. It involved a person submitting a bogus claim on a single or several occasions, while twenty per cent of insurance fraud in the low-income earners' insurance market is attributed to occupational fraud, according to the ACFE (200) occupational fraud is defined as fraud committed by employees of a company. This type of fraud is lading because employees take advantage of loop holes with insurance companies' systems. Insurance companies offering services to low-income earners in Zimbabwe hardly invest in artificial intelligence. This compounded by low levels of education amongst low-income earners provides an easy opportunity. Five per cent of insurance fraud is related but slightly different from occupational fraud in internal insurance fraud is when a firm commits fraud against itself. Insiders, and managers, commit this sort of fraud by concealing facts and conspiring with external stakeholders such as policyholders, agents, and employee representatives (Babalola, 2009). External insurance fraud, unlike internal insurance fraud, is perpetrated by third-party service providers. External insurance fraud includes providing false statements and including fraudulent claims of the policyholder, such as consumer fraud, counterfeit insurance in the purchase of an insurance policy, or claim-making through fraudulent coverage or payment (Yusuf, 2010). Insurance intermediaries assist in the procurement of insurance services and provide services to both insurance companies and individuals that meet the insurance coverage requirements. In the past, insurance agents and brokers were the two types of middlemen and usually, an average of three per cent (3%) of insurance crime in the low-income earners sectors is attributed to this type of fraud.

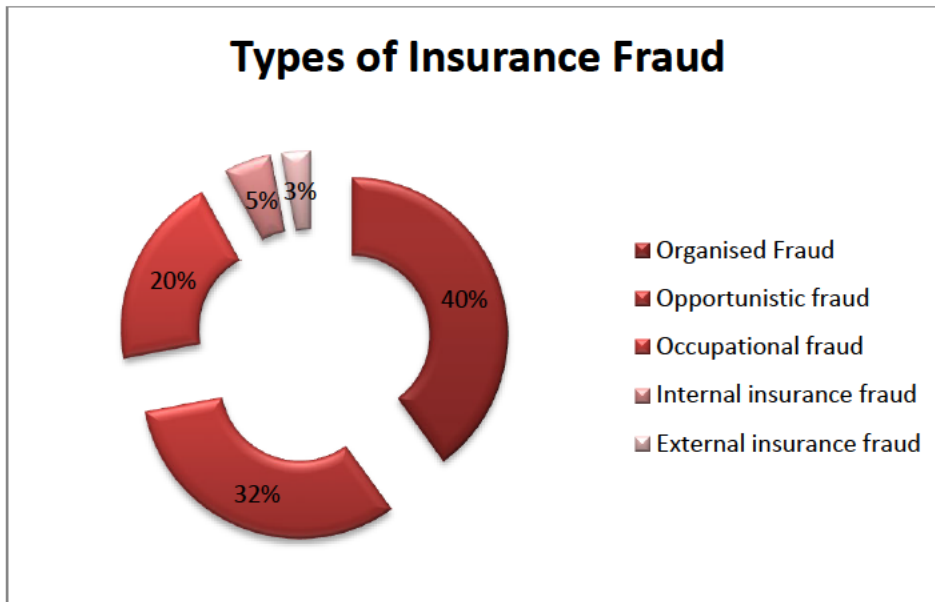


Figure 6.1: Types of Insurance Fraud

(Source: Owner Compilation)

The scope of credit card, identity, and cyber fraud makes it the most pervasive crime and costs the insurance sector. Fraud has reached pandemic levels in Zimbabwe and should be considered a national security issue. Tax credit and student loan fraud against the public sector are examples of how terrorist organizations and lone actors use fraud to fund their operations. This study's findings indicated that a wide range of cyber-attacks is increasingly focusing on the insurance business. Ransomware is a major threat to the industry, much like it is too many other sectors. If networks were infiltrated, ransomware operators would be able to identify and obtain policy information and security requirements for their cyber insurance clients. Because policyholders are more likely to pay ransoms if their insurers cover it, cyber insurance coverage for ransomware attacks, particularly coverage of ransom payments, makes organisations more appealing targets to organised criminal syndicates. This study also found that, in addition to encrypting files and holding them for ransom, the threat of data disclosure has now become a typical component of ransomware assaults and an extra layer of extortion. Given the risk of losing customer trust and confidence, the legal or regulatory consequences of releasing customer or employee data, threats to dump compromised files which contain information of security value on the dark web for further exploitation by other criminal syndicates are made in an attempt to pressure victims to pay a ransom. In addition to serving enterprise clients, insurance companies also hold a wealth of private information

about each of their retail clients that can be misused by criminals for fraud and other nefarious activities. For those who are enrolled with the National Social Security Authority (NSSA), the Social Security numbers and dates of birth are the most crucial data points. These are essential components in identity theft schemes like bogus credit applications. Attackers have had several possibilities to take advantage of the COVID-19 epidemic, especially when targeting healthcare institutions because they are particularly affected by this public health emergency. As an example, the creation of COVID-19 inoculation and testing records has provided attackers with access to a new data set of patient records. Such compromised critical information may be exploited primarily by fraudsters, but state-sponsored threat actors may also use it to assist their investigation and intelligence operations.

6.4 Findings on Factors Enhancing Insurance Fraud

This study identified two categories of factors enhancing insurance fraud in the micro insurance sector. The two categories are internal and external factors. Tables 6.2 and 6.3 below display frequencies of the two factors. An analysis of the factors exhibits that both internal and external factors, causes of insurance fraud are suggested to be influencing factors with ninety-five point eight per cent (95.8%) of respondents confirming that external factors are the most contributing factors of insurance fraud while eighty point eight per cent.

Tables 6.2 and 6.3: External and Internal Factors Enhancing Insurance Fraud.

Table 6.2 Are external factors are the most contributory factors of micro insurance fraud compared to internal factors			Table 6.3 Are internal factors the most contributory factor of micro insurance fraud compared to external factors		
	N	%		N	%
Strongly Agree	320	95.8%	Strongly Agree	270	80.8%
Agree	11	3.3%	Agree	59	17.7%
Neutral	1	0.3%	Neutral	1	0.3%
Disagree	2	0.6%	Disagree	2	0.6%
Strongly Disagree	0	0.0%	Strongly Disagree	2	0.6%
			Disagree		

(Source: SPSS)

Confirmatory factor analysis (CFA) is a multivariate statistical procedure that is used to test how well the measured variables represent the number of constructs. Based on Figure 5.5 and Table 5.5 CFA allowed for the assessment of fit between observed data and a prior conceptualized, theoretically grounded model that specifies the hypothesized causal relations between latent factors and their observed indicator variables. Figure 5.5 categorised causes of insurance fraud into two broad categories namely external and internal factors. External factors comprised of Opportunity (-.041), Initiator (.034), Conspiracy (.102), Reward (.160), Justification (-.109), Access (.235) and Safety (-.184). While internal factors included Remuneration (-.086), Internal Control System (-.043), Artificial Intelligence (.021), Prior Employment Vetting (.198), Training and Development (.030), Awareness (.169) and Intelligence Sharing (-.169). An examination of the loading pattern to determine the factor that has the most influence on each variable. Loadings close to -1 or 1 indicate that the factor strongly influences the variable. Loadings close to 0 indicate that the factor has a weak influence on the variable. Some variables may have high loadings on multiple factors.

In terms of external factors, findings from the study confirmed there are eight (8) factors that contribute or enhances insurance fraud. External factors that contribute to insurance fraud are factors independent from the insurance company excluding remuneration Table 6.1 above, an examination of Zimbabwe Republic Police criminal dockets on insurance fraud, the eight factors that contributed to insurance fraud or most prevalent were:

1. Reward also remained an important motivator. Whether perceived or real reward, all these saved as a motivator to commit insurance fraud. Criminal particularly organised crime syndicates are driven by a desire to achieve a reward from their criminal activities. The rewards may vary from monetary, religious or political.
2. Existence of an opportunity, opportunity referred to circumstances within an insurance company that allows insurance fraud to occur. There are various opportunity factors that can be exploited by organised crime syndicates which may vary from policies, governmental, economic, legislation, law enforcement and social and technological changes (Albanese, 2003).
3. Conspiracy and access to the systems of the targeted insurance company are also two important factors. . Conspiracy is when two or more persons

agree to commit a crime together and is a necessary component of organised crime. An agreement between at least two people is required for an act of insurance fraud; an agreement with oneself makes the act impossible (The Criminal Procedure and Evidence Act, 2016). Conspiracy should lead to an agreement. The agreement should be entered into with the objective of obtaining a pecuniary or other meaningful benefit, whether directly or indirectly (United Nations Office on Drugs and Crime, 2012). It is important to note that research findings unearthed that conspiracy also leads access. One of the members of the organised crime syndicate should have access by way of either being an employee, agent or policyholder. The syndicate might also have sub access by recruiting or working with individuals within the targeted insurance company. Access, in this case, means access to operating procedures, financial status of the company, internal systems and the weaknesses of the system that can be manipulated.

4. Safety refers to the possibility of the criminal act to be detected and compromised before, during or after the act. Organised crime syndicate usually carry out an assessment to determine the level of safety. They usually try to avoid criminal acts that are highly monitored and with a high possibility of detection (Criminal Investigation Department, 2020).
5. Justification, the criminal conduct should be justified irrespective of the criminal(s) acting in isolation or as a group. Justification may vary from thinking that what they are doing is right, and money obtained maybe used to finance other criminal activities either locally or externally.
6. Initiator. An assessment of criminal records indicated that any for of fraud needs to have initiator. The initiator is usually the brains behind the crime and the strategist well. In an organised crime group, the initiator is usually the team leader and is the centre of the crime and recipient of information from various sources with regards to the targeted insurance company.
7. Access. Transnational criminal networks can generate huge sums of money, and like any other business, they require access to organization operations systems, employees and the international financial system to conduct their complex and far-reaching operations. Security on most

micro-insurance service providers is physical security, rather than tracking and seizing the money being earned by the criminal networks.

The seven identified factors work as an integrated front and the absence of one factor may negatively affect the decision of the whole criminal act irrespective of the type of insurance fraud. Eighty per cent of respondents strongly agreed that these factors contribute to insurance fraud, with further confirmation that the seven factors are almost equally important.

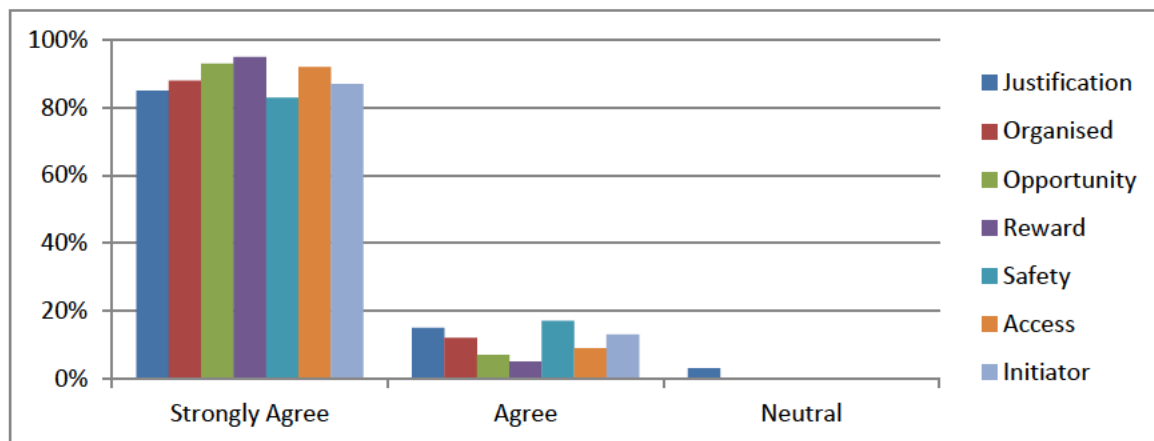


Figure 6.2: External Factors Enhancing Insurance Fraud

(Source: Owner’s Compilation)

However, Figure 6.3 below, factors internal to the organisation that also plays an equally significant role in enhancing insurance fraud. Inequitable remuneration. Employee remuneration plays a pivotal role in pushing the employees to commit fraud in the work place also referred to as occupational fraud. Organised crime syndicates prefer to work or operate with disgruntled employees and hence they invest their time in scouting for such employees in the micro insurance service providers. In that regard, inequitable remuneration has over years increasingly become an operational risk for insurance companies. Organisations in the modern Zimbabwe both public and private have since shifted their focus to focus more on remuneration equity. The 2008 economic crisis in Zimbabwe was characterised by hyperinflation and compromised remuneration equity (Labour and Economic Development Research Institute of Zimbabwe, 2019). Inequitable remuneration has been identified as one of the leading factors that trigger employees in insurance companies to engage in fraud. Remuneration plays a pivotal role in any organisation to motivate and incentivise

performance, loyalty and employee's retention (Larkin & Leider, 2012). Poorly remunerated employees in insurance companies are highly likely to engage or are easily enticed to commit insurance fraud related crimes (Insurance and Pension Commission, 2018). Respondents to this study confirmed that profiling and validation of data supplied by policy holder both existing and potential is a practical solution. Profiling and validation is the process of extrapolating information about a person based on known traits or tendencies in order to fully identify and know the person, determine whether the person is involved in illegal activities, and predict behaviour based on specific characteristics (President's Department, 2020). Profiling and validation may act as a first line of defence amongst policy holders while prior employment verifications and criminal vetting are also complementary counter measures. However, noted is that ninety per cent of micro insurance service providers in Zimbabwe do not invest much of their time in profiling and validation of policy holders and prior employment background checks. Further, lack of capacitation of employees through training and development, initiatives for training and development are educational activities carried out within an organization with the goal of enhancing an individual's or a group's performance on the job. The majority of these programs focus on improving a worker's knowledge and skill sets as well as inspiring more drive to improve work performance, hence a tactical instrument for enhancing corporate results through the implementation of internal educational initiatives that promote staff development and retention. Insurance service providers therefore view training and development as a cost rather than an investment, in that regard sixty-five per cent of employees in the micro insurance sector lacks industry specific capabilities such as fraud identification and investigations. Hence this has made micro insurance service providers susceptible to insurance fraud. Training and development is also complemented by public awareness. Public awareness is the degree to which the general public is aware of the significance and ramifications of insurance fraud.

Further to this, micro insurance service providers should also take responsibility in investing in the industry specific technology and also strengthening internal control systems such as policies and procedures. A swift analysis of micro insurance service providers revealed that little is done in investing in artificial intelligence and also internal control systems. Respondents to this study confirmed that artificial intelligence and internal control systems are all pivotal in combating insurance fraud, but contrary to this notion, micro insurance service providers hardly invest in artificial intelligence but rather they even conduct their

business manually, with poor internal control measures hence accounting. One last component which this study identified is intelligence sharing. Respondents noted that intelligence sharing is a component of countering insurance fraud that can be explored by micro insurance service providers. This was recommended on the basis that there is no connection between intelligence services and insurance companies while intelligence services monitor organised crime syndicates. Intelligence sharing in the long run will effectively counter insurance fraud since insurance companies will share notes particularly watch list of individuals and individuals involved in insurance fraud.

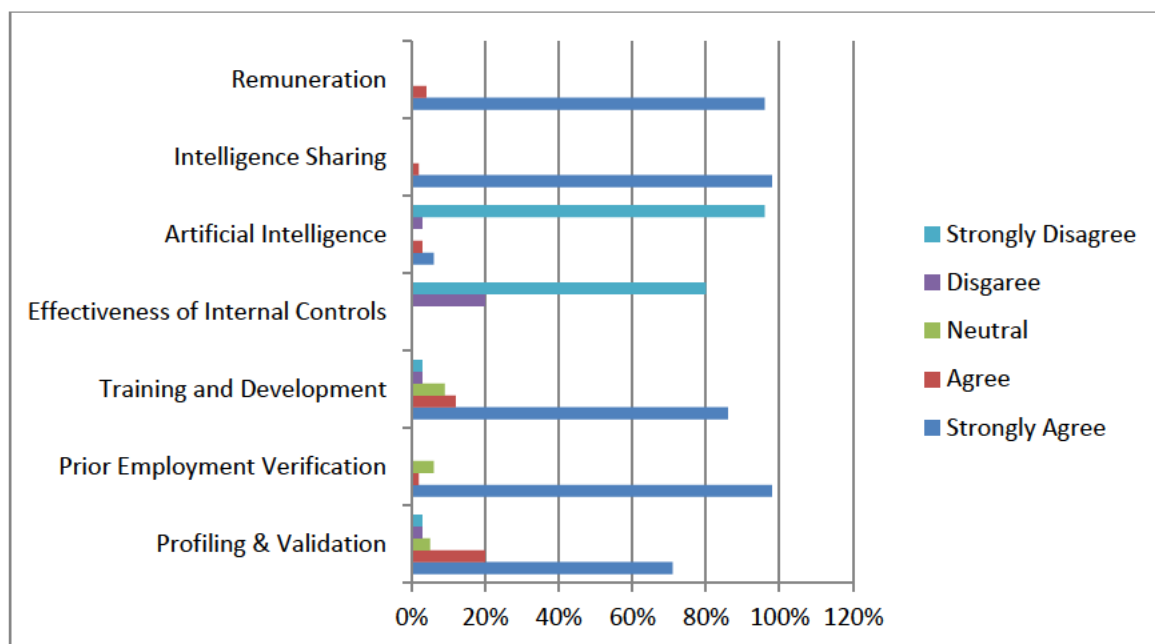


Figure 6.3: Internal Factors Enhancing Insurance Fraud

(Source: Owner’s Completion)

6.5 Findings on Organised Crime Syndicates Operations in the Insurance Industry

Findings are that insurance fraud in the low-income earners market is highly perpetrated by organised crime syndicates and resultantly, this attributes to the increase of premiums. Because of Zimbabwe's ineffective state power and governance, organized crime and criminal networks have grown, which has made it more difficult to establish a successful state. The Zimbabwe Anti-Corruption Commission (ZACC) (2020) estimated that the cost of money lost to insurance fraud in Zimbabwe is estimated USA nine billion dollars per year, this excludes unreported cases. The main objective of these organised criminal syndicates is to swindle the insurance industry to fund their criminal and terrorist activities around the world. Document inspection of classified intelligence with the security intelligence apparatus

revealed that there are sixteen well-established organised crime syndicates which are targeting insurance companies. The findings further confirm that these organised crime syndicates have regional and international links in which money obtained in Zimbabwe is electronically transferred to subunits for onward usage in other criminal activities. Further, these organised crime syndicates are spread all over the ten provinces of Zimbabwe. Organised crime syndicates usually work as one front forming a transnational organized crime syndicate. Further findings are that transnational organised crime syndicates pose a clear, serious threat to national security, the threat, however, is not limited to a single nation, but also the international security, hence compromising public safety, health, democratic institutions and economic stability. Transnational organised crime groups' criminal activities are well coordinated, pre-meditated, concealed and lethal hence threatening human security. Continuous criminal operations by these groups subsequently lead to human rights violations and further undermine the socio-economic, cultural and political development of the affected societies (McDermott, 2015). Notably, organised crimes are dynamic and fluid, they adapt to the situation, changing with time and technology hence bringing about new and sophisticated crimes which are flexible and global in nature. The fact that organised crime syndicates can operate globally indicates relationships are formed amongst homogeneous crimes; this is achieved only when the syndicates overcome linguistic and cultural differences in their operations. Criminal activities with a global outlook are common in Latin America, Venezuela, Mexico, Bolivia, Colombia, Guatemala, Honduras, and Peru (McDermott, 2015). Whilst in Africa they include ungoverned space and war-torn areas such as Somalia, Ethiopia, Nigeria, the Democratic Republic of Congo (DRC), Afghanistan, Sudan, and Zimbabwe due to a lack of stringent countermeasures and involvement of political figures and intelligence officers. The involvement of organised criminal groups related to Islamic terrorist and insurgent groups such as Boko Haram in Nigeria, Al-Shabaab in Somalia, and Ansar al-Sunna Wa-Jama in Mozambique is one of the most concerning aspects of crime being financed by money obtained from insurance fraud.

According to the Global initiative against transnational organised crime (2020), in discussions about organised crime in Africa, the phrase "criminal networks" is frequently used to refer to the region's more adaptable and dynamic criminal organisations. In Africa, organised crime and criminal networks take on a variety of shapes that are mostly determined by the strength of the state and the extent to which political elites are personally involved in

them. Mafia-style organizations that are well-established and structured, like the hard-core gangs in South Africa's Western Cape, or militia-style operations engaged in 'taxing' local populations and economic activities, both licit and illicit. The most renowned criminal networks in Africa are those in the West, but there are a variety of other foreign criminal players looking for opportunities in Southern Africa as well. These rather loose but frequently quite effective criminal networks are located in the middle of the spectrum. On the other end are groups of criminally inclined business people who frequently operate under the guise of corporations such as the Guptas in South Africa, but who also enjoy various sorts of political protection. Illicit financial outflows, in particular, are a severe concern, but governance and regulatory reforms will be considerably more vital than law enforcement agencies suppressing illicit markets, given evidence of extensive coordination between police and criminals in several illicit markets. The study of illicit markets on the continent itself has made it evident that as globalisation and trade integration have expanded, so too has Africa's involvement in the world's criminal economy (Shaw, 2017). Since 2000, there has been a stronger and more consistent link between organised crime and Africa's conflicts, statehood, government, and society. Kleptocracy, illicit financial flows, illegal trade, and criminal activity have all evolved into toxic forces that worsen income disparity, prolong and escalate conflicts, degrade the environment, compromise human security and, ultimately, further marginalise the weak and the poor (Reitano & Hunter, 2018).

6.6 Findings on Insurance Companies Targeted by Organised Crime Syndicates

Laxity amongst microinsurance companies to invest in insurance fraud countermeasures remains a serious concern among insurance regulators and experts. This has, however, created numerous opportunities for organised crime syndicates in Zimbabwe. Organised crime syndicates according to the findings of this study are that the targeted insurance companies lack adequate insurance fraud countermeasures in terms of artificial intelligence and other relevant internal systems and procedures. Insurance companies mostly targeted by organised crime syndicates are the ones offered tenders by the Zimbabwean government, and contracts to offer various services to civil servants and government parastatals. According to the Zimbabwe Public Service Commission (2021), the government of Zimbabwe is the biggest employer in Zimbabwe with an estimate of an unaudited three point two million employees. These insurance companies are offering diversified insurance services to government employees as well as the government itself. The services vary from health,

funeral, vehicle, home, and life insurance coverage, amongst others. Organised crime syndicates target these insurance companies taking advantage of laxity in security and systems. Mobile technology has revolutionised the financial service sector which has also enabled micro insurance to be remotely distributed across the world, even to low-income earners in the most remote areas of Zimbabwe hence additional clients from the three-point two million. This mobile technology through mobile money and e-wallet or eco-cash as it is known in Zimbabwe has opened up new channels for insurance claims even for the unbanked population (Technology in Micro Insurance, 2019). Finding by this study pointed out that, failure by the insurance industry to employ advanced proactive controls designed to detect potential fraudsters during and after the application process is a leading concern. Further, there are various artificial intelligence systems, applications and software that are commercially available for insurance companies to deploy to counter insurance fraud. This study has acknowledged that there are six elements namely poor screening process of employees before employment, lack of employee training on counter insurance fraud, poor internal controls, lack of artificial intelligence, lack of awareness to policyholders and lack of collaboration with state security intelligence apparatus. The lack of these presents an opportunity for organised crime syndicates.

A greater part of insurance companies in Zimbabwe, nearly sixty-five per cent, hardly believe that insurance fraud is a greater threat to the industry, but rather blame poor performance on international sanctions imposed on Zimbabwe by Britain and America. This mind set has had an impact on the performance of insurance firms and classes of business over the years, forcing customers to bear the financial penalties while insurers deal with the harm to their brand and reputation. Regardless of the hazard, the majority of insurance companies do not and will not devote resources to combat insurance fraud. Another finding noted with concern is that insurance companies have failed in the past to invest in insurance fraud countermeasures that can be instigated internally or externally. The study unearthed that most insurance companies are manually processing claims with only a few aided with computer systems. Also, the insurance companies are not working with the national intelligence agency to counter insurance fraud.

6.7 Findings Regarding Legislation to Counter Insurance Fraud

Legislation and policy were identified as a component that can aid in the prevention, detection, and response to insurance fraud, for example by defining clear laws, rules, and

criteria, enabling insurance companies to gather information, and report it to the relevant authorities, as well as enforcing fines and recovering fraud losses. Research participants were requested to input and comment on the effectiveness of current legislation in countering insurance fraud in Zimbabwe. Recent anti-fraud campaigns in Zimbabwe exhibited that smart use of both criminal and administrative remedies, as well as policy design, can disrupt, minimise and prevent insurance fraud. An initiative in Zimbabwe to combat insurance fraud exhibits how legislation, policies, an interagency collaboration between the intelligence and police, and the tactical application of both criminal and administrative measures can thwart and prevent insurance fraud. Seven acts that directly apply to insurance fraud were recognised by the respondents as needing to be revised to be effective in combating insurance fraud. Among the statutes identified were the Insurance and Pension Commission Act, Chapter 24:21, the Insurance Act, Chapter 24:07, the Anti-Corruption Act, Chapter 9:22, the Criminal Law, Chapter 9:23, the Criminal Procedure and Evidence Act, Chapter 3:1, the Prevention of Corruption Act, Chapter 9:16, and the Money Laundering and Proceeds of Crime Act, Chapter 9:24. It was noted with concern that the use of legislation is an effective preventative countermeasure; however, the realignment with the new Zimbabwe constitution will make these Acts more effective. It was commented that it is insufficient to have fully constitutional legislation on paper without assurances of constitutional behaviour, particularly from institutions supporting democracy. In line with insurance fraud, due to a lack of evidence and regulations that could result in the punishment of insurance fraud offenders, different incidences of insurance fraud in Zimbabwe go unpunished; therefore, government initiatives are made to address these varied legislations gap issues. Although this is very admirable, it can be proven that several policy gaps have been uncovered over the years and are still unresolved. The government's efforts to realign the legislation and policies about fraud and corruption are admirable considering that these Acts are all-encompassing in terms of investigating, evidence collection and prosecution of perpetrators (Insurance and Pension Commission 2019).

6.9 Findings with Regards to the Role of Security Intelligence in Countering Insurance Fraud

The respondents identified that insurance fraud is thriving because intelligence-based policing is non-existent in the field of insurance fraud. The respondents affirmed that the national intelligence organisation has a pivotal role to play in countering insurance fraud. In the

questionnaire, respondents noted that insurance fraud and fraud, in general, require a proactive approach usually deployed by security intelligence organisations rather than the reactive approach deployed by the Zimbabwe Republic Police which only acts once a crime has been done. Further findings are that, organised crime is quickly becoming a lucrative industry in Africa, according to the United Nations Office on Drugs and Crime (2010), generating USA dollars eight hundred and seventy billion, or one point five per cent of world's gross domestic product. This is a criminal business that also has the potential to destabilise Africa. In Mozambique, Somalia, and Angola, organised crime continues to undermine peace and human security, and human rights are being abused, damaging societies' economic, social, cultural, political, and civil growth (INTERPOL, 2018). This threat alone is of great magnitude and requires extensive intelligence gathering before initiating countermeasures. Tactics and tradecraft deployed by security intelligence namely covert operations, recruitment of sources and informants, surveillance, infiltration and penetration and continuous profiling and monitoring of organised crime group members were deemed restrictive and were recommended by research participants. In Zimbabwe, there are three security intelligence organisations namely the Central Intelligence Organisation, which operates under the cover name of the President's Department, this is a secret service organisation that is responsible for the collection, analysis, exploitation of information and covert countermeasures in support of national security initiatives and other security organisations, namely Zimbabwe Republic Police and Zimbabwe National Army, Military Intelligence Directorate complements. Findings pointed out that the role of national security intelligence organisations is to detect and thwarts threats to national security and interest emanating internally or externally. Their targets and mandate are directed by the President and they intervene at whatever level once national security and interest are threatened hence their deployment in dealing with matters of insurance fraud perpetrated by organised crime syndicates is not questionable. Contrary to this, research findings are that micro-insurance service providers who have been working closely with the Zimbabwe Republic Police have since abandoned working with the police on suspicion that the individuals within organised crime groups are police officers. Corruption in the judiciary system in Zimbabwe has further worsened the situation in which insurance companies fail to secure a conviction for arrested perpetrators. In that regard, findings further confirmed that ninety-two per cent of research participants recommended that micro-insurance service providers prefer a proactive, preventative approach in dealing with insurance fraud hence the need to seek services.

6.10 Conclusion

The discussion in Chapter Six of this study focused on a critical review of issues related to the primary study findings, which were reported in the previous chapter, and it provided a comprehension of the research findings, of interest, was the desire by the insurance service providers recommending a counter insurance fraud design that is rather preventative and proactive. Hence, this chapter's emphasis was on the discussion and interpretation of the findings in light of the study's goals and within the framework of already-existing theory and data. Research findings had to cut across the most important aspects of the study, dissecting across the demographic characteristics, identifying factors influencing insurance fraud in the low-income earners market, threats posed by organised crime, state of countermeasures in the insurance companies and the role of security intelligence in countering insurance fraud.

The last chapter provides a summary of the main findings, conclusions and recommendations of the research study.

CHAPTER SEVEN

CONCLUSION AND RECOMMENDATIONS

7.1 Introduction

The threat of insurance fraud in the micro insurance sector continues to gobble finances invested in the development of micro insurance service delivery in Zimbabwe and the insurance industry at large. Organised crime syndicates, being on the forefront in peddling various types of insurance fraud crimes, have been opportunistic, taking advantage of security lapses within micro insurance service providers and also the strength of technological advancement at their disposal. In that accordance, amongst the objectives of this study was to investigate the causes of micro insurance fraud and also recommend counter measures. This was against the backdrop that insurance fraud in the micro insurance market is affecting low income earners who are already incapacitated. The chapter starts out with an overview of the research findings, highlighting how each discovery relates to the study's objectives. Following that, proposals for an integrated approach that insurance firms might use to combat insurance fraud are made. After that, recommendations are made for potential areas for further study.

7.2 Main Findings and Conclusions of the Study

7.2.1 Research Conclusion Conceptual Framework

The conceptual framework of this study illustrated the expected relationship between the independent and dependent variables. It defined the relevant study objectives in sync with the research process to draw coherent conclusions. Conclusions drawn from this study from a sample of three hundred and twenty-six research participants are that organised crime syndicates are exploiting internal weaknesses and capitalising on external strengths to advance their criminal activities. Hence confirming that insurance fraud in the microinsurance sector can emanate internally or externally. Chapter five (5) of this study unearthed that organised crime syndicates are motivated by various factors to commit insurance fraud. Financial rewards and poor internal security systems within micro-insurance service providers are among the motivators. Further, there is growing concern over the threat of fraud related crimes in the low-income earners market. Cases of insurance fraud in micro insurance are increasing daily (Crime watch Zimbabwe, 2020). The level of threat and the terrain of organised crime in Zimbabwe have altered significantly over the past few years,

largely as a result of technological improvements. Organised criminal organisations have embraced new technology and incorporated them into their methods of operation, creating new crime models. Across the gamut of insurance fraud offences, organised crime groups' use of technology affects criminal activity, most importantly concealment of the identity of perpetrators. The presence of organised criminal syndicates operating in the microinsurance sector is one concerning feature of insurance fraud. It is critical to comprehend the behaviour and motivation of these criminal organisations to combat them. Five elements can be applied by insurance companies to counter or contain insurance fraud. Figure 7.1 below, understanding the sources and causes of insurance fraud is one thing but designing countermeasures is the most important thing. Conclusions are that, for effective counter insurance fraud in the microinsurance market, there are five areas that the insurance regulatory authority in conjunction with insurance companies needs to consider. Eighty per cent (80%) of the research participant recommended an overhaul of the insurance company's internal policies procedures while ninety per cent recommended an assessment of technological requirements, and artificial intelligence to complement internal policies. Further, ninety-two per cent of the research participant also concluded that occupational fraud in the microinsurance market was also rife, with the employee working in isolation or collaboration with organised crime syndicates, in that regard it was concluded that prior employment background checks and employee capacitation through training and development would internally aid counter occupational insurance fraud. Seventy one per cent research participant raised a concern over the lack of participation by the micro insurance industry in awareness, with the recommendation that the insurance industry should play a pivotal and leading role in public awareness particularly on issues to do with threats and effects of insurance fraud and also government awareness, recommending effective legislation that capacitates the judicial system, insurance regulatory authority, the police and security intelligence to effectively identify the threat, investigate and arrest perpetrators. Considering the surreptitious nature of insurance fraud, ninety-one per cent of the research participants recommended a proactive, restrictive approach to counter insurance fraud, however, this required security intelligence lead operations in numerous ways that may include intelligence sharing on organised crime watch list, profiling and criminal clearance of suspects, restrictive surveillance and covert operations to dismantle and eliminate organised crime groups.

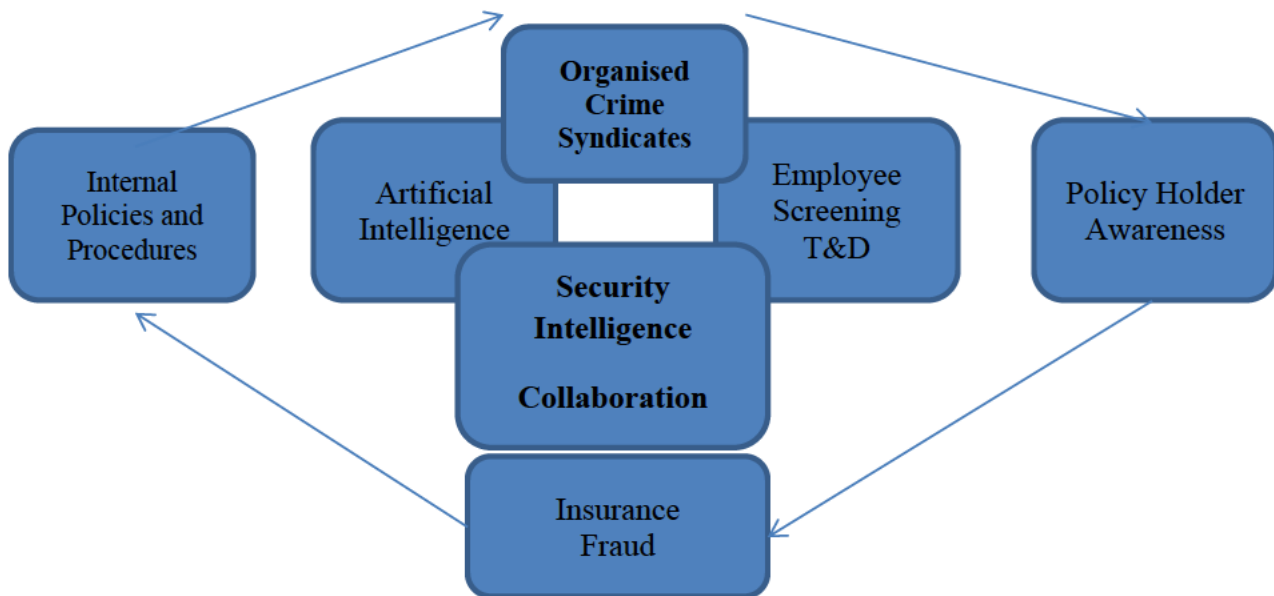


Figure 7.1 Research Conclusions Conceptual Framework

Source: Author's compilation

7.2 Recommendations

Insurance companies in the low-income earner's sector have recognised the need to always be one step ahead of fraudsters. A realisation that organised crime within the insurance industry can be easily formed amongst employees, policy holders' and criminal individuals. Recent developments are that micro-insurance service providers across the globe are alive to the fact that increased collaboration with external stakeholders such as the security intelligence apparatus and regulatory authorities has since encouraged coordinated thinking and strategising, and a collaborative approach to the management and containment of the threat of insurance fraud in the microinsurance segment (Roberts 2019). With recent developments in the insurance industry, micro-insurance service providers have since advocated a "zero tolerance to insurance fraud" policy as a potent deterrent to "would-be" opportunity seekers and organised fraudsters. Irrespective of whether the insurance industry has declared Zimbabwe an insurance fraud-free zone, insurance fraud remains a highly surreptitious crime, very difficult to detect, peddled on highly secure and secret circles of organised crime syndicates in which identities of the perpetrators are concealed. The United Nations office on drugs and crime (2021), acknowledged that organised crime is increasingly changing and becoming an elusive and fluid phenomenon that can go undetected. The benefits of globalisation, such as encryption software, easier and faster online communications, mobile banking and online money transactions, and the internet of things,

have allowed organised criminal groups to thrive, diversify, and grow their operations while operating secretly and from diverse places across the globe. In that regard, micro-insurance service providers and general insurance service providers are not spared from the global menace of insurance fraud, considering their lax security (Roberts, 2019).

In light of the above, research objectives number one to four of this study namely to:

1. Investigate the causes of insurance fraud in the low-income sector in Zimbabwe;
2. Evaluate the impact or threat level of insurance fraud targeted at low-income earners to national security and interest;
3. Assess the role of security intelligence organisations in countering insurance fraud in the low-income sector in Zimbabwe; and
4. Prescribe other strategies that can be fused with security intelligence to counter insurance fraud in the low-income sector in Zimbabwe.

Literature has recommended various approaches for micro insurance service providers to counter insurance fraud. Pivotal to these recommendations is the need for an integrated all-encompassing approach that insulates an individual insurance company from all forms of insurance fraud while also the entire insurance industry is equipped with capabilities to detect, investigate and thwart the threat of insurance fraud. Empirical research objective number four (4) was to prescribe strategies that can be fused with security intelligence to counter insurance fraud in the low-income sector in Zimbabwe

The focus of the recommendation was to equip the micro-insurance service providers with proactive capabilities meant to detect and thwart insurance fraud amongst customers or policyholders, amongst employees, designing internal security measures fused with artificial intelligence to detect insurance fraud, developing initiatives to educate the general public with regards to threats and consequences of insurance fraud and also working in liaison with security intelligence. Figure 7.1 below suggested that the insurance industry and insurance companies ought to have CEPSI (360) capabilities to counter insurance fraud. The CEPSI (360) capabilities should equip insurance companies with the capabilities to detect, prevent, sanction, investigate and redress insurance fraud. The acronym CEPSI abbreviates for

Customers, Employees, Participation, Systems and Intelligence. The three-sixty (360) implies a total and from all angles insulation of the insurance company.



Figure 7.2: Customers, Employees, Participation, Systems and Intelligence 360

Source: Owner's Compilation

The CEPSI 360 presupposes that insurance fraud is a systemic and complex issue, a threat that requires a collaborative approach to counter. The various national experiences of fighting insurance fraud suggested that the efforts of insurers and other relevant stakeholders should be focused on five key areas namely:

- 1) Consumer or policy holder
- 2) Employees
- 3) Awareness
- 4) Internal policies and technology
- 5) Security intelligence

7.2.1 Customer /Policyholder

Policyholders, that is, customers of any insurance company, remain pivotal in the success of the company. The insurance companies offering services to low-income earners generate funds through premiums from millions of policyholders. Due to the long-term nature of the insurance relationship, funds from policyholders are crucial to the survival of the insurance company. Microinsurance service providers minimise insurance fraud, for starters are expected to attract free policyholders (Insurance and Pensions Commission, 2020). Historically, organised crime syndicates found it easy to penetrate an insurance company through the purchase of a policy. Furthermore, individuals with criminal intentions, individuals with criminal records and known fraudsters, and organised crime syndicates have gained entry into insurance companies in the same way. This was made possible by security lapses within micro-insurance service providers in which insurance policy applicants are not subjected to rigorous screening and validation that is meant to detect and weed out criminal threats from the start. It is recommended that micro-insurance service providers subject both current and potential service providers to:

- Profiling and validation
- Criminal clearance
- Vetting
- Awareness
- Incentivising

7.2.1.1 Profiling and validation

Profiling and validation is the process of extrapolating information about a person based on known traits or tendencies to fully identify and know the person, determine whether the person is involved in illegal activities, and predict behaviour based on specific characteristics (President's Department, 2020). Profiling of a potential policyholder is initiated by the policy application form. The application form should be the most important form between the insurance company and the policyholder; sometimes it is referred to as the proposal form (The Economic Times, 2021). The application should capture information with regards to the applicant which includes names, age, pictures, address, education, employment and other relevant background information. The application form should also go a step further to gather information concerning names, contact details and addresses of family members, trade references and family doctors. Further to this, the application form should request the attachment of national identity cards, proof of income from the bank and proof of house ownership or confirmation of lease. The insurance company should however validate all the information provided by the applicant. Validation can be done at the registrar general's office or its equivalent, the Zimbabwe Republic Police's Criminal Investigation Department (ZRP), or the registrar of companies in the case of corporations seeking insurance services. Validation is a collaboration done with the issuing authority to determine the authenticity and legality of any government document and information issued by the possessor. At this stage, insurance companies will be able to detect and weed out fake documents. Though this might seem a laborious process, it is an important process, regarded as the first line of defence.

7.2.1.2 Criminal Clearance

A police criminal clearance is an official document issued by the police stating whether or not any criminal convictions have been recorded against an individual (Criminal investigation department, 2018). The Zimbabwe Republic Police (ZRP)'s Criminal Investigation Department (CID) is in charge of producing these clearances through its Criminal Records Office, which works in collaboration with the Central Criminal Bureau. Criminal records and confirmed convictions are handled by the two sections. Insurance firms should work in liaison with these departments. Further, a serious recommendation is that microinsurance service providers should equip their personnel with the capabilities to collect fingerprints from possible applicants, which can subsequently be forwarded to the appropriate body for criminal clearance. Usually, figure prints are indexed with a criminal's name, try if crime and

facial identification linkage. Hence an attachment of figure prints forms by the applicant can easily give an insurance company the capacity to know the historical crimes committed by the applicant. It will be, however, the decision of the insurance company to forgo applicants with a crime such as traffic offences, but should seriously evaluate clients or applicants with crimes related to fraud, money laundering, human, drugs and arms trafficking, terrorism, robberies and cybercrimes.

7.2.1.3 Vetting

Vetting is an examination and critical appraisal designed to deter undesirable elements from becoming part of an organisation in any way and impede such elements (undesirable) from having access to classified material information that will aid their criminal endeavour. There are three types of vetting, namely initial, continuous and extended vetting. Insurance companies can request the National Intelligence department to do the vetting on their behalf, particularly insurance agents operating abroad and foreign applicants. Intelligence officers attached to the insurance and pension commission can easily conduct the vetting. Vetting as a defence mechanism should not only be limited to policyholders but should stretch to employees, insurance agents and brokers and service providers. Initial vetting is done during the application phase be it if a potential policyholder, service provider or employee. An insurance company must know what kind of threat is posed by each applicant. While continuous is meant to detect and determine if one has not yet gone rogue, contaminated or recruited by organised crime syndicates. Extended vetting will stretch to family, relatives and friends to determine if they are not a security risk.

7.2.1.4 Awareness

Policyholder awareness is knowledge or perception of a situation or fact. Insurance fraud is evolving so must be awareness. Insurance fraud awareness should be done at the industry level by the insurance and pension commission targeting insurance companies and by insurance companies targeting policyholders. Fraud awareness, both at industry and company levels, contributes towards reducing the risk of insurance fraud. Awareness can be periodically done through social media alerts, formal communication through letters, newsletters and emails, training and public citizen awareness (Insurance and Pension Commission, 2021). Equipping both the industry and the public with knowledge and information concerning threats of insurance fraud and consequences will to some extent deter organised crime syndicates from engaging policyholders and employees.

7.2.1.5 Incentivising

Incentivising is motivation and encouragement for doing something that is perceived to be correct. Insurance companies need to come up with innovative insurance products that incentivise policyholders to not be involved in any insurance fraud-related cases. Such rewards and incentive schemes should focus on redirecting policyholders to avoid and report all forms of insurance fraud. In comparison to other businesses, an insurance firm has a particular requirement to match economic objectives with preventative behaviours that might result in cheaper premiums and a competitive edge in the marketplace. Policyholders can be dynamically compensated through behaviour-based pricing, which encourages positive behaviour and creates a virtuous shared-value cycle between risk reduction and profit (Pfitzer, 2017).

7.3 Employees

This study recommended that insurance companies can reduce the threat of insurance fraud through the capacitation and management of employees. Manna (2008) suggests that employee capacitation and management are strategically necessary for developing employees that can deliver organisational strategic goals. Minimisation of insurance fraud remains an organisational priority. It is therefore prudent for insurance companies to weed out undesirable and criminal elements amongst employees' prior recruitment. This can be achieved through rigorous background checks before employment. Employee background checks are a review of a potential employee's record compiling criminal, financial, and commercial historical background information. It also determines whether an applicant is unqualified and suitable on analysis of the historical criminal record, credit history and work history. When hiring personnel for positions of trust, insurance companies must conduct background checks to ensure that they are hiring a risk-free individual. Such background checks should be undertaken during the pre-employment phase for possible employees and are the primary means through which companies obtain information about potential employees from sources other than the applicants themselves (Proctor, 2021). This phase usually entails contacting applicants' prior employers, supervisors, co-workers, the police, and educators to verify previous employment history and acquire information about the individual's knowledge, skills, abilities, and character. This study recommended:

Prior employment verification: This validates the applicant's employment with the specified employers, including dates of employment, position held, and any extra information

concerning performance rating, the reason for departure, and suitability for employment. An in-depth analysis particularly focusing on issues related to misappropriation, fraud and corruption at work. Such vices render a possible applicant unacceptable.

Educational verification: This verifies the applicant's claimed qualifications, including the years of attendance and the degree or diploma attained, with the indicated educational institutions. Educational or qualification verification apart from determining a match between job requirements and qualifications, insurance companies should check for inconsistencies in programs studied and the authenticity of the certificates.

Criminal history: Criminal history checks are also important when trying to contain insurance fraud. This includes an examination of criminal convictions and the sort of crime committed. The following elements could be considered for applicants with a criminal record:

- The crime's nature and its connection to the position.
- The amount of time that has passed since the conviction.
- The number of convictions (if more than one).
- Whether hiring would put the insurance company, its workers, and its customers at an unacceptable risk.

Credit history: It verifies the credit history of a potential employee. This search is necessary for positions in insurance businesses that require the management of corporate funds, direct contact with clients, and the processing of cash or credit cards.

Terror and organised crime watch list: Keeping a terror and organised crime watch list of possible workers is very important. It is a requirement for security positions and jobs that include managing business funds and handling cash or credit cards.

Checking court records: This is done to determine if the candidate has ever been or is currently involved in any legal procedures. This is critical in identifying the suitable individual who can devote their entire attention to the job profile being given.

Reference checks: This helps to establish an employee's integrity, dependability, consistency, and personality when compared to job requirements.

7.3.1 Employee Training and Development

Employee training and development is an endeavour to strengthen an individual's ability to perform through learning, either by changing attitude or by extending skills and knowledge. Training and development improve employee future performance by focusing on and

enhancing organisational skills that are tailor-made to the specific requirements of both the job and the organisation. An organization's skills deficiencies should be identified through a needs assessment before beginning a staff training and development program. It is essential to assess first in light of organizational capabilities requirements. The difference is what is known as the skills gap. The training goals will be based on the skills gap. However, it is important to create training objectives that take organizational capabilities into account. Adjusting suspicious fraudulent claims, evaluating claims, handling claims best practices, conducting claims investigations, considering insurance professionals' ethics, and comprehending insurance fraud challenges are some examples of insurance fraud-related organizational competencies. The insurance company may opt to consider internal or external training. Insurance companies that seriously invest in the training and development of employees invest in skills development that positively impacts productivity in all forms. A business gains from investing in the knowledge and skills of its employees by having more productive and efficient workers. Training and development improve personnel and organisational capacities. According to Peters (2006), there are four stages of training and development, each with its own set of learning outcomes:

- Organisational operating procedures. These organisational-specific focused functional skills. This gets an individual up to speed on financial, accounting, marketing, strategy, information technology, economics, operations, and human resource management challenges.
- Internal and external elements. Understanding context and strategy, as well as how organizational processes interact, involves taking into account factors including societal changes, political and social values, global issues, and technological advancements are also important skills for employees within insurance companies.
- Motivation. If the management of an insurance firm does not have a solid understanding of motivational concerns, staff and clients may be impacted, and enticed to join organised crime syndicates.
- Reflective skills. It is essential for employees to be dedicated to their work and to establish priorities for their work and personal endeavours. This is an important skill as well.

7.4 Participation in Awareness

The insurance companies, insurance agents and the public have continuously and unconsciously hampered efforts by the government of Zimbabwe to counter insurance fraud. Policyholders and other related institutions are not yet aware of the prevalence of insurance fraud. Insurance fraud continues to be a concern to national security and is the second most expensive white-collar crime; hence it is critical that customers and relevant institutions are made aware of this. It has negative impact to the government, the economy, and policyholders, with compliant policyholders facing increased insurance premiums as a direct consequence of insurance fraud. In that regard, more should be done by insurance companies to focus on countering insurance fraud in their initial interaction with potential policyholders. Awareness is a powerful initiative against insurance fraud. A policyholder who is aware of the different types of fraud and vulnerabilities involved can dramatically decrease chances of insurance fraud. Insurance companies should distribute more information to policyholders about what constitutes fraud, as well as spelling out the consequences. Insurance companies should take note that there are two types of awareness, that is, internal awareness and external awareness. Internal awareness focuses on employees and agents while external awareness focuses on policyholders and the general public. Awareness should be initiated at three levels. The first level is the initial insurance fraud awareness. This is awareness that is initiated for the first time an insurance company hires an employee, engages an agent and offers a contract with a policyholder. Secondly, continuous insurance fraud awareness, that is, the insurance company implement a plan to periodically update employees, policyholders and agents with regards to on-going trends on insurance fraud. Thirdly, liaison awareness is level that is mainly concerned with public awareness and liaison with relevant government departments such as regulatory authorities, intelligence and security and the police. Insurance companies can directly participate in public and industry awareness through combined workshops, road shows and media campaigns. Insurance companies also have a pivotal role to assist security organisations and regulatory agencies in conducting insurance fraud threat assessment, cost of insurance fraud, statistics gathering and construction of watch list. When insurance companies intend to participation in awareness, they should come up with a clearly defined strategy that addresses five (5) aspects such as:

- 1) Identifying the insurance fraud awareness needs
- 2) Insurance fraud awareness goals and objectives
- 3) Targeting the audience

- 4) Communication methodology
- 5) Determining frequency of awareness

7.5 Systems

Insurance companies are generally organised into five broad departments that are claims, finance, legal, marketing and underwriting. Quite succinctly, insurance companies make money through underwriting profit; investments; and reduced overall claims expense. Examining each of these potential profit centres helps to explain insurer motivation in countering insurance fraud through investment in artificial intelligence systems and internal control systems.

7.5.1 Artificial Intelligence Systems

The ability of insurers to combat insurance fraud has grown tremendously in direct proportion to technological improvements. Data analysis has been changed by the emergence of capabilities such as data visualisation, claims to score, and predictive modelling. Other advancements have improved procedure and workflow, such as fast internet access to massive volumes of public-records data and automatic compliance reporting. The Zimbabwean government and insurance companies are more motivated than ever to combat insurance fraud by adopting artificial intelligence detection systems. Currently, there is a rise in the deployment of innovative technological solutions in the global insurance industry aimed at tackling insurance fraud. Insurance companies should integrate efficient artificial intelligence systems and procedures for preventing insurance fraud. Such an initiative demonstrates effective financial management and good corporate governance (The Chartered Institute of Public Finance and Accountancy, 2015). The rise to a more globalised interconnected, online and the internet of things has transformed the traditional, physical business environment into an intangible online business, including that of insurance services (Schuvab, 2016). This transformation has given organised crime syndicates leverage to swindle insurance companies, considering that micro-insurance service providers hardly invest in innovative technological countermeasures. It is highly recommended that micro-insurance service providers should find it necessary to fuse the insurance process and technology, a term is known as InsurTech or insurance technology (Bibi, 2018). The Coalition against Fraud (2020) in their report on artificial intelligence and insurance fraud have identified artificial intelligence systems as the most possible insurance technology that could be adopted to counter insurance fraud. The Coalition against Fraud (2020) defines

artificial intelligence as data technological systems that routinely screen for fraudulent claims using predictive analytics logic driven by advanced data modelling methodologies and statistical algorithms. It is advised that providers of microinsurance make investments in artificial intelligence. Over time, artificial intelligence systems have progressed beyond recognising human danger signs to reporting and data visualisation, automated corporate procedures, and predictive analytics. The investment has shown to be effective in forecasting sophisticated and changing fraud tendencies that insurers are facing as a result of rising digitalization. A variety of artificial intelligence tools that is currently available on the market for commercial use may be used by insurance companies, including but not restricted to:

Detection of anomalies: The user establishes baselines for KPIs related to actions or occurrences, and then defines thresholds with anomaly detection. When a given measure's threshold is exceeded, the event is reported. Outliers or anomalies are used to identify existing, unique, and previously unknown fraud tendencies.

Network analysis: In the insurance industry, organised fraud involving several linked claims and entities still exists. To combat organised fraud rings, insurers are focusing on new, extremely sophisticated capabilities for analysing social networks and identifying linkages and patterns. Network link analysis has been beneficial in detecting organised fraud operations by modelling linkages between entities in both the claims and new business acquisition phases. While link analysis is not new to insurance fraud investigations, artificial intelligence's capacity to analyse large amounts of data and link it to individuals and organised criminal gangs is a valuable countermeasure.

Analysis of images and vision: Computers can use image analysis to determine whether the claimant in the photo or on the ID card is the insured person. It can also determine whether the identity card being presented is legitimate and has not been used in any previous fraudulent claims, downloaded from the internet, or tampered with in any way.

Web crawling: A new aspect of text mining is the ability to evaluate data and information available on social networking sites. On Facebook, Twitter, Snap Chat, Instagram, LinkedIn, Craigslist, and other social media platforms, non-meritorious claims of information and evidence can be found. While this social media strategy is cutting-edge, several insurance companies are mining and analysing unstructured text data in useful ways with the help of software.

Predictive modelling: Insurance data scientists utilise predictive modelling. This is a type of machine learning to create predictive models that generate fraud propensity ratings. New

business applications and claims are automatically rated for their potential of being fraudulent as data is input and updated.

Geospatial insurance: Geospatial insurance gives an insurance business the ability to get highly detailed insights into a geographical area's insurance needs. Types of insurance policies are likely to be acquired in a specific geographic location or ZIP code, for example. Geospatial insurance technology also allows for a more precise distinction between real and fraudulent claims, offering reliable data for statistical analysis in the future.

Case management: During the investigative process, the case management system is in charge of weeding out inefficiencies. The system assures compliance by keeping a detailed paper trail for each case, documenting all activities and events as they occur. It enhances operational efficiency even more by providing investigators with immediate access to the data they need to make better conclusions. Complex cases, growing fraud, and tight regulatory requirements are posing new obstacles for investigation teams. The case management system is a fully customisable fraud management tool that automates triage, assignment, and compliance reporting, resulting in increased productivity and efficiency.

7.5.2 Internal Control Systems

Insurance businesses can use a variety of artificial intelligence tools to combat insurance fraud. The insurance business is increasingly supporting the idea of incorporating artificial intelligence. Most insurance firms now supplement the effort with internal control mechanisms rather than depending solely on technology. The blending of artificial intelligence and organisational internal control systems increases the capabilities and refines detection and counter insurance fraud techniques. Artificial intelligence tools employed may not be enough to deter all prospective criminals. The micro-insurance service provider should deploy and make sure that both artificial intelligence and internal control systems are in place to detect and combat insurance fraud. Internal control systems are policies and procedures that complement organisational effective and efficient operations. Internal control systems cover approval and authorisation processes, access constraints and transaction controls, account reconciliations, and physical security. These procedures usually include the division of roles, and checks and balances to reduce risk (Chartered Institute of Management Accountants, 2008). The association of British Insurers (2016) prescribed that, when an insurance company is establishing internal control systems, the systems should be non-negotiable and mandatory. In that regard, internal control systems must be:

- Annually documented and reviewed.
- Conduct assurance reviews of critical risks throughout the business and regions to detect 'gaps.'
- Identify weaknesses in the system and take corrective action to remedy them; and implement procedures for reporting suspected fraud.
- Organise regular fraud management team meetings.
- Determine which sections of the company are at risk.
- Provide management with information on fraud that has been detected and trends (and develop narratives on any regulatory concerns).
- Develop a flexible fraud response plan by using scenario planning.
- Conduct internal audits to ensure that procedures are working properly.
- Apply what you have learned from previous fraud cases.
- Do additional vetting of workers in high-risk sectors to prevent internal fraud.

Staff should be made aware of the necessity to protect data, the existence of internal fraud indicators, whistle-blower procedures, and the penalties of internal fraud as part of internal control systems. The departing point for an insurance company to come up with airtight internal control systems is to develop a sound ethical culture within an organisation. The foundation for a high or low-fraud-risk environment is the culture of an insurance company or any organisation. According to the Chartered Institute of Management Accountants (2008), micro-insurance service providers that have seriously considered assessing where they stand on ethical issues have found that having high ethical standards has long-term benefits. This creates confidence amongst clients, vendors, employees, and the community knows what they are dealing with. Once an insurance company is committed to establishing a sound ethical culture, Recommendations are that there should be:

- A mission statement that refers to the quality or, more unusually, to ethics; and defines how the organisation wants to be regarded externally;
- Clear policy statements on business ethics and anti-fraud, with explanations about acceptable behaviour in risk-prone circumstances;

- A route through which suspected fraud can be reported;
- A process of reminders about ethical and fraud policies, for example, annual letters and or declarations;
- An aggressive audit process which concentrates on areas of risk; and
- Management who are seen to be committed through their actions

7.6 Intelligence

In developing economies such as Zimbabwe, the low-income cover has been classified as a strategic human security issue meant to combat poverty. However, insurance fraud continues to escalate in insurance companies offering low-income coverage, particularly civil servants. This has become a threat to the sustainability of the low-income cover market. The Zimbabwe national intelligence organisation has adopted the concept of human security. The human security approach broadens and changes the scope of intelligence and security from territorial, state-centric security to the security of people. Microinsurance is the “the protection of low-income earners against specific perils in exchange for regular premium payments proportionate to the likelihood and cost of the risk involved” (International Association of Insurance Supervisors, 2007). Insurance fraud is classified as a serious predicate offence under Zimbabwe's Money Laundering and Proceeds of Crime Act (2013) and international standards. A predicate offence is “an illegal offence, which has the potential to provide funds for other crimes such as money laundering and financing of terrorism” (Bibi, 2018). It is against this background that the national intelligence organisation is mandated, from the directive of the President of Zimbabwe, to intervene since insurance fraud is compromising both national security and national interests. The role of the Zimbabwe national intelligence organisation is to “detect and thwart threats to national security and interest emanating internally or externally”. The national intelligence organisation can counter insurance fraud by executing six (6) out of the many diversified functions, namely gathering intelligence, intelligence collaboration and sharing, countering international organised crime, support to criminal justice and regulatory agencies, covert action and enforcement.

The collection of intelligence: Gaining a complete grasp of a threat to national security and interests is the aim of intelligence gathering. The evaluation and investigation process can help intelligence agents make decisions about how to deal with risks and what preventive

measures to implement. Organised crime groups have a history of highly technical, stealthy, concealed and sophisticated insurance fraud schemes. The national intelligence organisation is equipped with a range of tools that can be used for intelligence collecting, including:

- Secret human intelligence sources, that is, people who can supply confidential information about an investigation's target;
- Static and mobile surveillance, such as following and or observing targets;
- Monitoring and interception of emails or phone calls, for example, communication interception;
- Bulk personal data and datasets containing information about a large number of people can be accessed in a targeted way to identify or find information about the subject of interest;
- Intrusive surveillance, such as putting eavesdropping devices in someone's home or car; and
- Interfering with equipment, such as secretly accessing computers or other devices.

Intelligence collaboration and sharing: Collaboration and exchange of intelligence are essential elements of anti-insurance fraud operations in the age of globalisation. Collaboration with other security forces, foreign but not hostile intelligence agencies, international insurance agencies, Interpol, governments, customs and immigration officials, insurance industry experts, and academics will go a long way in educating the world about how insurance fraud is evolving and being perpetrated by organised crime syndicates around the world. Intelligence briefs on organised crime syndicates' watch lists, trends and tactics deployed by organised crime syndicates, intelligence alerts on possible movement of organised crime syndicate members, the technology used by criminals, and possible areas of operations are examples of accurate intelligence that would have been collaborated with independent external sources.

Countering organised crime: Intelligence and security organisation is also mandated to counter threats posed by organised crime syndicates. Organised crime syndicates have since identified the insurance industry as an easy source of money to finance their criminal activities. Money obtained through insurance fraud is being used to finance arms and drugs trafficking, corrupt government officials and state security agents, terrorism, purchase of encryption software and hardware, and money laundering amongst other vices. The need to

counter organised crime arises when a threat to domestic security and interests is detected; as its influence on the economy and the political systems of the country.

Support to criminal justice and regulatory agencies: An intelligence organisation, apart from providing information and intelligence to other law enforcement agencies and regulatory authorities, is also heavily involved in policy and legislation research. It is the primary responsibility of an intelligence and security organisation to advice and influence policy and legislation formulation and changes in a direction that fosters national security.

Covert action: This is a highly secret and swift operation conducted by an intelligence and security organisation. The operation exhibits a muscular approach rather than diplomacy but is less expensive and obtrusive than military force. Three categories of covert action include propaganda and disinformation, political action and paramilitary action. Intelligence and security organisations can mount covert operations to campaign worldwide against individuals or groups involved in organised insurance fraud. It can also cause political action that acknowledges the threat of insurance fraud and arouse the political will to discredit and counter insurance fraud. Finally, through paramilitary action, the intelligence and security organisation can deploy officers to identify, track and cause the arrest or elimination of organised crime syndicate members and even confiscate or destroy both software and hardware used to carry out insurance fraud.

Enforcement: The intelligence and security agency is the most globally represented law enforcement organisation in the world, with officers stationed all over the world, and is best positioned to tackle transnational crime. The organisation's crime-fighting capabilities are provided by highly trained special agents, fraud investigators, investigative specialists, intelligence research specialists, forensic accountants, and other experts. Furthermore, the organisation has built a global network that includes foreign law enforcement agencies, immigration agents, and Interpol over the years. Cooperation with regional and international counterparts against organised criminal organisations, dismantling those criminal groups both within and outside Zimbabwe, and pursuing and supporting efforts to prevent those organisations' operational success will go a long way toward combating insurance fraud. The Zimbabwe Republic Police is responsible for maintaining law and order throughout Zimbabwe, protecting people and property, and preventing and investigating crime. However, through Presidential declaration, the national intelligence organisation can be empowered to maintain law and public order in matters that affect the entire country. If other law enforcement agencies and regulatory bodies are executing legislation and counter-insurance

fraud tactics advocated at the national level, this enforcement role would overlap. Since the national security intelligence, since it has an oversight role, insurance companies can work with the security intelligence in perusing the monitoring and implementation of counter-insurance fraud programs implemented by the industry and government.

7.7 Limitations

Efforts and modalities were put in place to ensure that the research addresses the research questions and objectives of this study. The empirical results of this study should be considered in light of the following limitations:

- i. The research was limited to insurance businesses and the insurance industry in Zimbabwe to determine the threat of insurance fraud to national security and national interest. It is not comparative research with regional or worldwide studies in other countries. The concentration on Zimbabwe is just a microcosm of the bigger picture of insurance fraud at the international level;
- ii. Furthermore, this study did not consider conducting a causality test to establish a direct relationship between insurance fraud and organised crime syndicates; or the relationship between insurance fraud and the performance of an insurance company. This was not done due to limited quantitative data on insurance fraud perpetrated by organised crime syndicates. A usual norm is that insurance fraud is being perpetrated by individuals, policyholders or insurance agents. The aspect of insurance fraud is a serious organised crime that requires further exploration;
- iii. Though the Ministry of State Security had cleared and granted the researcher access to classified intelligence on activities of organised crime syndicates, access to highly classified documented intelligence particularly classified as “top secret” was limited as well as access to information regarding syndicates under serious investigations was restricted;
- iv. This limitation restricted the researcher from classified information about the modus operandi being used by organised crime syndicates. A clear understanding of the modus operandi deployed by organised crime syndicates is crucial in designing countermeasures; and
- v. Much research on insurance fraud is being focused on insurance companies in general without segmentation. There is limited study on insurance fraud in the microinsurance market segment. Further research is required on issues affecting the operations of

micro insurance service providers and an assessment of the socio-economic and political impact of such a threat.

7.8 Conclusion

The endeavour of microinsurance companies to come up with effective insurance fraud countermeasures within microinsurance service providers should not be underestimated considering the mutating nature of insurance fraud crime perpetrated by organised crime syndicates. The level of micro-insurance penetration is one glaring distinction between emerging and developed nations. With about fifty per cent of the world's population surviving on less than five USA dollars daily. These low-income earners are the most at risk of being harmed by a natural disaster and are also the most vulnerable. Small business owners and farmers are especially at risk because an incident could rob them of their meagre assets and even the most basic needs. The hazards that low-income earners confront internationally are specifically addressed through microinsurance. Although there is no single, universally accepted definition of microinsurance, practically all parties involved concur that, at its foundation, microinsurance is insurance for low-income earners, and people with modest incomes. A noticeable increase of insurance companies venturing into micro-insurance services considering the potential, huge client base. The study revealed that there is zeal amongst low-income earners to take up some form of insurance. However, this zeal has been over the years devastated due to increasing levels of insurance fraud peddled by organised crime syndicates.

In determining issues to do with motivation amongst organised crime syndicates to target insurance companies offering service to low-income earners, the structural equation modelling was applied and the results confirmed a causal effect of internal and external variables that contributed to the causes of insurance fraud in low-income earners. With that confirmation, insurance companies offering services in the low-income sector should, however, design administrative innovations that counter all forms of insurance fraud. The administrative innovation should look into a complete overhaul of internal systems and procedures, human capital management and recruitment procedures. Further, considering organised syndicates have gone technical, it's also important that insurance companies fuse their operations with artificial intelligence. Artificial intelligence gives insurance companies technical capabilities to detect insurance fraud in cyberspace. Importantly, insurance companies need to also tap into capabilities that can be sourced externally. An assessment

and evaluation of cases of insurance fraud and fraud in general exhibits that fraud is a highly secret and deceptive crime hence it requires intelligence-lead countermeasures. The role of security intelligence is quite pivotal in detecting, investigating and eliminating insurance fraud.

“Actuaries should be part of the conversations that create better information technology that is capable of handling the large volumes of data generated in the provision of microinsurance. This will drive the design of suitable risk management plans, accurate sensitivity, stress test and adequate reserving” Mildred Areeta | President, the Actuarial Association of Uganda.

REFERENCES

- Abell, P. (2000). "Rational Choice Theory." Pp. 252–77 in *Companion to Social Theory*, edited by Turner Bryan S. Oxford: Blackwell.
- Adams, J. (1966). *Wage Inequities, Productivity, and Work Quality*. *Industrial Relations*, 3, pp, 9- 10.
- Adams, J. S. (1963). Inequity in social exchange. In L. Berkowitz (Ed.), *advances in experimental psychology* pp. 267-299. New York: Academic Press.
- Adams, J. S. (1963). Toward an understanding of inequity. *Journal of Abnormal and Social Psychology*, 67, pp 422-436
- Agostinho, P. & Cherry, C. 2014. The Significance of Claims Fraud In Micro Insurance And A Statistical Method To Channel Limited Fraud Identification Resources. Presented at the Actuarial Society of South Africa's 2014 Convention 22–23 October 2014, Cape Town International Convention Centre
- Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), Pp. 179 – 211.
- Al-Madi, A. (2012). The Impact of Corporate Social Responsibility on the Performance of Pharmaceutical Companies in Jordan. *International Journal of Business and Social Science*.
- Al-Zawahreh A & Al-Madi F. (2012). The Utility of Equity Theory in Enhancing Organizational Effectiveness. *European Journal of Economics, Finance and Administrative Sciences* (46).1.
- Albanese, J. (2015). *Organized Crime: From the Mob to Transnational Organized Crime*.
- Albanese, J. (2015). *Illegal Gambling & Organized Crime: An Analysis of Federal Convictions. Trends in Organized Crime*.
- Albanese, J. (2003) *Transnational Organized Crime*
[Internet: <http://Dx.Doi.Org/10.14135/9781483349091.N3>.Downloaded on 5 February 2022]
- Apel, R. (2013). "Sanctions, Perceptions, and Crime: Implications for Criminal Deterrence." *Journal of Quantitative Criminology* 29: pp 67-101
- Arachchilage, N.& Love S. (2014). *Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective*. *Computers in Human Behaviour* 38: pp304-312.
- Arunga, A. (2012). *Micro-Insurance Risk Management: A Survey of Insurance Companies in Kenya*. Unpublished Project, United States International University, Nairobi.

Arunga, A. (2012). Risk Management Practices: A Survey of Micro-Insurance Service Providers in Kenya. *Internationals Journal of Financial Research* 4(1).

Asare, T. (2006). Beating Occupational Fraud through Awareness and Prevention. Acfb Working Paper No10.

Association of British Insurers (2016). Statement of best practice for critical illness. [Internet: <https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2016/protection/statement-of-best-practice-for-critical-illness-cover-dec-2016.pdf>. Downloaded on 5 February 2022]

Association of British Insurers. (2011). Statement of best practice for critical illness.[Internet: <https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2011/protection/statement-of-best-practice-for-critical-illness-cover-dec-2011.pdf>. Downloaded on 10 February 2022]

Association of British Insurers. (2012). Statement of best practice for critical illness. [Internet: <https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2012/protection/statement-of-best-practice-for-critical-illness-cover-dec-2012.pdf>. Downloaded on 21 February 2022]

Association of Certified Fraud Examiners. (2020). Report to the Nation: 2020. [Internet: <https://legacy.acfe.com/report-to-the-nations/2020/docs/RTTN-Government.pdf>. Downloaded on 6 December 2021]

Association of Certified Fraud Examiners (2010). Report to the Nation on Occupational Fraud. [Internet:<https://legacy.acfe.com/report-to-the-nations/2010/docs/RTTN-Government.pdf>. Downloaded on 6 December 2021]

Association of Certified Fraud Examiners (2017). Report to the Nation on Occupational Fraud. [Internet:<https://legacy.acfe.com/report-to-the-nations/2017/docs/RTTN-Government.pdf>. Downloaded on 6 December 2021]

Association of Certified Fraud Examiners (Acfe) (2019). Report to the Nations. 11th edition of the largest global study on occupational fraud. London. [Internet:<https://legacy.acfe.com/report-to-the-nations/2019/docs/RTTN-Government.pdf>. Downloaded on 6 December 2021]

Association of Certified Fraud Examiners, (2010). Report to The Nations On Occupational Fraud and Abuse, 2010 Global Fraud Survey'. Austin. <https://legacy.acfe.com/report-to-the-nations/2010/docs/RTTN-Government.pdf>. Downloaded on 6 December 2021]

Association of Certified Fraud Examiners, (2012). Report to the Nations on Occupational Fraud and Abuse, 2012 Global Fraud Survey'. Austin, TX: ACFE. <https://legacy.acfe.com/report-to-the-nations/2012/docs/RTTN-Government.pdf>. Downloaded on 6 December 2021]

Association of Certified Fraud Examiners. (2019). Red Flags for Detecting Insurance Fraud, pp. 1-33.[Internet: <https://www.acfeinsights.com/acfe-insights/6-common-red-flags-fraud>. Downloaded on 12 September 2022]

Association of Government Accountants (2021). AGA Professional Development Training 2021 (PDT). Nashville Tennessee. [Internet; <https://m.eventsinamerica.com/events/aga-professional-development-training-2021-pdt-association-of-government-accountants/business/investment-finance/ktpy3e77ch419gnv>. Downloaded on 7 November 2022]

Association of Insurance Commissioners of United States of America (2019). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education*, 23(4), pp.521–533.

Attorney General. (1992). Guidelines for Undercover and Sensitive Operations Unit. Undercover Operations, November 13.

Australian Criminal Intelligence Commission (2019). Examination of the Australian Criminal Intelligence Commission Annual Report 2019-20. Commonwealth of Australia.

Australian Criminal Intelligence Commission (2019). Micro insurance and the Threat of Organised Crime. Paper presented at the ninth conference on Micro insurance in Zimbabwe. 10-18 June, Harare, Zimbabwe.

Australian Organised Fraud and Intelligence Group. (2017). Fraud and Financial Crime Management. Reduce Risk, Protect Against Financial Crime and Meet Regulatory Compliance.

Australian Organised Fraud and Intelligence Group. (2017). The Global Business of Organised Crime 2017 Report. ACIC.

Awang, Z. (2012). A Handbook on SEM. 2nd Edition. Terengganu: Universiti Sultan Zainal Abidin.

Awang, Z. (2015). SEM Made Simple: A Gentle Approach to Learning Structural Equation Modelling. Bandar Baru Bangi: Mpws Rich Publication.

Awang, Z., Afthanorhan, A., Mamat, M. & Aimran, N. (2017). Modeling Structural Model for Higher Order Constructs (Hoc) Using Marketing Model. *World Applied Sciences Journal*, 35(8), pp.1434-1444.

Babalola, S. S. (2009). Determinants of Unethical Business Behaviour among Owner–Managers. *Journal of Human Values*, 15(1), pp.61–75.

Bartling, B. and von Siemens, F. A.: (2011). Wage inequality and team production: An experimental analysis, *Journal of Economic Psychology* 32(1), 1–16.

- Baron, J. N. and Kreps, D. M.: (2013). Employment as an economic and a social relationship, in R. Gibbons and J. Roberts (eds), *Handbook of Organizational Economics*, Princeton University Press, pp. 315–341.
- Backham, D., Wahl, J. & Rose, S. (2010). *Executive's Guide to Solvency II*: 46 Wiley and Sas Business Series, Rose, Stua.
- Bagozzi., F & Yi'. S (2000). Examining Individual Board Member Behaviors in Nonprofit Sport Governing Bodies. *Nonprofit and Voluntary Sector Quarterly*, 50(2), 458–472.
- Baker, B. (2015). *The Breakthrough Insurance Agency: How to Multiply Your Income, Time and Fun*.
- Bandura, A. (1977). Self-Efficacy—Toward a Unifying Theory of Behavioral Change. *Psychological Review*, 84, pp.191-215.
- Beattie, A. (2021). *The History of Insurance: From Ancient Babylonia to the American Colonies*. Investopedia. Usa
- Becker, G. (1976). *The Economic Approach to Human Behavior*. University of Chicago Press, Chicago.
- Biener, C. & Eling, M. (2012). Insurability in Micro Insurance Markets: An Analysis of Problems and Potential Solutions. *Geneva Papers On Risk & Insurance - Issues & Practice* 37(1): pp.77-107
- Biener, C. Eling, M. (2016). *The Geneva Papers on Risk and Insurance. Issues and Practice* 37 (1), pp77-107.
- Boyer MM. (2000). Centralizing Insurance Fraud Investigation. *The Geneva Papers on Risk and Insurance Theory* 25(2):159-178
- Bowen, G. A. (2009). Document Analysis as A Qualitative Research Method. *Qualitative Research Journal*, 9(2), pp.27-40.
- Brody R. (2010). "Beyond the Basic Background Check: Hiring The “Right” Employees", *Management Research Review*, 33(3): pp 210-223.
- Brown, T. A. (2015). *Confirmatory Factor Analysis for Applied Research (2nd Ed.)*. The Guilford Press.
- Browne's, J. (2019). "The Definition of Insurance: Implications for A Health Insurance Demand Model" Charles Fuhrer Washington National Insurance Co
- Bryman, (2014). Red Flags for Detecting Micro Insurance Fraud in Zimbabwe, 1-33.
- Bullens, A.C.J. Houtekamer. A. Van Dam, V. & Kadijk, S. (2006). Paper on Micro Insurance. Asian Knowledge Centre for Mutual Insurance' Askmi.

- Button, M., Pakes, F. & Blackburn, D. (2016) 'All walks of life': A profile of household insurance fraudsters in the United Kingdom. *Secur J* 29, pp501–519.
- Carmines, E. G., & Mciver, J. D. (1981). Analyzing Models with Unobserved Variables: Analysis of Covariance Structures. In G. W. Bohinstdt, & E. F. Borgatta (Eds.), *Social Measurement: Current Issues* pp. 65-115. Sage.
- Carrell M & Dittrich J. (1978). Equity Theory: The Recent Literature, Methodological Considerations, and New Directions. *Academy of Management Review*, 3, pp.202-210.
- Carrell, M.R. and Dittrich, J.E. (1978) Equity Theory: The Recent Literature, Methodological Considerations, and New Directions. *Academy of Management Review*, 3, pp.202-210
- Catherine, M & Gretchen, R. (2006). *Designing Qualitative Research*. Thousands Oaks: Sage Publication. 4th Edition. New York, Ny: Routledge
- Central Intelligence Agency (2018). Interagency Intelligence Briefs on Organised Crime. Bulawayo, Zimbabwe. [Internet: <https://globalinitiative.net/wp-content/uploads/2018/08/TGIATOC-Zim-Organised-Crime-Report-WEB.pdf>. Downloaded on 1 May 2022]
- Central Intelligence Agency, (2018). The Emerging Role of Intelligence in the Mordern World. [Internet: <https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/pdf/GPO-INTELLIGENCE-6.pdf>. Downloaded on 1 March 2022]
- Central Intelligence Agency, (2019). C.I.A Wold Factbook 2019-2020. Skyhorse.
- Central Intelligence Agency. (2019). Fraud and Organised Crime in Zimbabwe. Intelligence Briefs. USA.
- Chamberlain., D. Hougaard., C. & Bester, H. (2009). What Is Micro Insurance and Why Does It Matter? Centre for Financial Regulation and Inclusion.
- Chitando, W. (2019). Brief on activities of artisanal miner's income. Harare: Zimbabwe's Ministry of Mines and Mining Development
- Cho, H., Lee, P & Shin, C. (2019). Becoming A Sustainable Organization: Focusing On Process, Administrative Innovation and Human Resources Practice. *Journal of Economics and Administration Sciences* (22): pp.456-479.
- Chow, M. Min, J. Biese, K & Mccord, M. (2019). Technology in Micro Insurance. How New Developments Affect the Work of Actuaries.
- Churchill, Q. (2006). Insurance in Developing Countries: Exploring Opportunities in Micro insurance. Lloyd's Micro Insurance Center: London. (1-38.)

- Churchill, C, Dalal, A & Ligh J. (2017). Impact Insurance Working Paper #18: Pathways Towards Greater Impact: Better Micro Insurance Models, Products and Processes For Mfis. The Ilo's Micro Insurance Innovation Facility.
- Churchill, C. & Mutual, M. (2012). Protecting The Poor: A Micro Insurance Compendium Vol. Ii, Geneva: International Labour Office and Munich Re Foundation
- Churchill, C. & Mutual, M. (2012). Protecting the Poor. A Micro Insurance Compendium Volume I. Germany.
- Clapper, J. (1995). Defence Intelligence. United States Intelligence Community.
- Classified Security Intelligence Brief (2012). Intelligence brief on organised crime and fraud. Harare. President's Department Head Quarters.
- Clarke, R.V. (1997). Situational Crime Prevention: Successful Case Studies. Albany, NY: Harrow and Heston. p. 229.
- Coalition against Insurance Fraud (2015), Insurance fraud may be leveling off. Fraud Data.
- Coalition Against Insurance Fraud (2017). Insurance fraud may be leveling off, Coalition Against Insurance Fraud
- Coalition Against Insurance Fraud. (2019). Globalisation of Insurance Fraud Statistics. Barcelona, Spain
- Cohen, J. (2013). Statistical Power Analysis for the Behavioral Sciences. Routledge Academic.
- Collins, A & Holton, K. (2004). Benefits of Training and Development For Individuals And Teams, Organizations, And Society. *Annual Review of Psychology* (60)1, pp.451-74
- Costanza, R. (2014). The value of the world's ecosystem services and natural capital. *Nature* 387, pp.253–260
- Consumer Council of Zimbabwe (2016). Annual Report 2016/2017. Harare.
- Consumer Council of Zimbabwe (2017). Low income earners Safety Nets. Propose model Towards Improved Social Services for Low Income Earners. Harare: Government Printers
- Cooper., D. & Schindler, P. (2013). Business Research Methods. 11th Edition, Mcgraw Hill, Boston.
- Cooper, D., & Schindler, P. S. (2008). International Edition: Business Research Methods
- Cooper, D.R. And Schindler, P.S. (2014) Business Research Methods. 12th Edition, Mcgraw Hill International Edition, New York.
- Counter Insurgency Training Manual (2017). Insurgency and Organised Crime.

Crabtree, B. F., & Miller, W. L. (1992). *Doing Qualitative Research: Multiple Strategies*. Thousand Oaks, Ca: Sage Publications.

Crano, D. Brewer, M, & Andrew Lac (2015) *Principles and Methods of Social Research*. Third Edition. Thousand Oaks, CA: Sage Publications.

Cresse, W. (1953). An investigation into the occurrence of corporate fraud. An empirical analysis conducted in Brazilian banking institutions

Cressey, D. (1950). The Criminal Violation of Financial Trust. *American Sociological Review* 15 (6): pp.738-743.

Cressey, D. R. (1971). *Other Peoples' Money: A Study in The Social Psychology of Embezzlement*. Glencoe: Free Press.

Cressey, D.R. (1971). *Other Peoples' Money: A Study in The Social Psychology of Embezzlement*, Free Press, Glencoe

Creswell, J.W. (2014). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches*. 4th Edition. Los Angeles, Ca: Sage Publications.

Creswell, J.W. (2014). *Research design: Qualitative, Quantitative, and Mixed Methods approaches*. 4th Edition. Los Angeles, Ca: Sage Publications.

Creswell, J.W. & Creswell, J.D. (2018). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches*. 5th Edition. Los Angeles, Ca: Sage Publications.

Creswell, J.W. & Creswell, J.D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th Edition. Los Angeles, CA: Sage Publications.

Criminal Investigation Department (2020). Annual Report on Organised Crime and insurance Fraud 2019/2020. Bulawayo. [Internet: http://www.zrp.gov.zw/index.php?option=com_content&view=article&id=102&Itemid=788. Downloaded on 8 March 2022]

Criminal Investigation Department. (2018). Evidence Presentation On Cases of Insurance Fraud To Insurance And Pension Commission. Harare. [Internet: http://www.zrp.gov.zw/index.php?option=com_content&view=article&id=102&Itemid=788. Downloaded on 8 March 2022]

Criminal Law and Codification Act of Zimbabwe (2000). Published in the Zimbabwe Gazette 314/2000. Government Printers. Harare. [Internet. <https://www.refworld.org/pdfid/4c45b64c2.pdf>. Downloaded on 1 January 2022].

Criminal Law Codification and Reform Act, (2017). Published in the Zimbabwe Gazette 3336/2017. Government Printers. Harare. [Internet. <https://www.refworld.org/pdfid/4c45b64c2.pdf>. Downloaded on 1 January 2022].

Criminal Procedure and Evidence Act (2019). Published in the Zimbabwe Gazette (126724). Government Printers. Harare. [Internet: <https://www.jsc.org.zw/upload/Acts/2011/0907updated.pdf>. Downloaded on 7 February 2022]

Crime watch Zimbabwe (2020). Zimbabwe Crime Statics. ZRP Criminal Investigation Department.

Dalal, R. (2014) Within-Person Variability in Job Performance: A Theoretical Review and Research Agenda. *The Academy of Management Journal* 52(5): pp.1051-1066.

David, L. (2010). Employee Theft: Determinants of Motive and Proactive Solutions" Unlv Theses, Dissertations, Professional Papers, and Capstones.

David, M. Dror, P & David, P. (2014). What Is Macro Insurance? Micro Insurance Academy. USA.

Davis, M. (2020). Strategies to Prevent and Detect Occupational Fraud In Small Retail Businesses: *International Journal Of Applied Management And Technology* 19(1), pp.40–61.

Deblon, Y & Loewe, M. (2011). The Potential of Microinsurance Protection. Handbook of Social Protection Systems pp.1213-134.

Deloitte (2020). Global Business Driven Human Resources Transformation: The Journey Continues.[Internet:<https://www2.deloitte.com/content/dam/deloitte/de/documents/human-capital/>; Downloaded On 29 March 2022.]

Denzin, N.K. and Lincoln, Y.S. (2005) Introduction: The Discipline and Practice of Qualitative Research. In: Denzin, N.K. and Lincoln, Y. S., Eds., Handbook of Qualitative Research, 3rd Edition, Sage, Thousand Oaks, pp.1-32.

Dillman, D.A., Smyth, J.D. & Christian, L.M. (2014). Internet, Phone, Mail, And Mixed-Mode Surveys: The Tailored Design Method. 4th Edition. Hoboken, Nj: John Wiley & Sons.

Dior, M.D. (2014) What Is Micro Insurance. *Ssrn Electronic Journal*.2434501.January 2014.

Dobie, M. (2012). Understanding insurance customer dishonesty: outline of a situational approach. *Journal of Business Ethics*, 61, pp.183-97.

Dollar. (2020). Report On the Commission of Inquiry into The Conversion of Insurance and Pensions Values. Harare. IPEC.

Dorminey J (2010). Beyond The Fraud Triangle: Enhancing Deterrence of Economic Crimes. *The CPA Journal*.

Dorminey, J (2012). The Evolution of Fraud Theory. *Issues in Accounting Education* Vol 27 (2): pp.555-579.

Douglas, J. E., & Burgess, E. (1986). Criminal Profiling from Crime Scene Analysis. *Behavioural Sciences and the Law*, 4, pp.401-421.

Dror (2018). Understanding insurance customer dishonesty: outline of a situational approach. *Journal of Business Ethics*.

Dubey, U., Kothari, D.P. & Awari, G.K. (2017). Quantitative Techniques in Business, Management and Finance: A Case-Study Approach. Boca Raton: Crc Press.

Dupuy, K & Neset, S. (2018). The Cognitive Psychology of Corruption. Micro-Level Explanations for Unethical Behaviour. Michelin Institute.

Dutton, W. H. (1999), *Society on the Line: Information Politics in the Digital Age* Oxford and New York: Oxford University Press.

Edward, P. (2015). Occupational Fraud: A Survey. Honours Theses. 281.

Edwards, J. R., & Bagozzi, R. P. (2000). On The Nature and Direction of Relationships Between Constructs and Measures. *Psychological Methods*, 5(2), 155–174. [Internet: <https://doi.org/10.1037/1082-989x.5.2.155>. Downloaded On 6 March 2022]

Elster, J. (1989). "Social Norms and Economic Theory." *Journal of Economic Perspectives*, 3 (4): pp.99-117.

Essentials of Structural Equation Modeling" (2018). Zea E-Books. 64. [Internet. <https://digitalcommons.unl.edu/zeabook/64brown>, 2015. Downloaded On 16 November 2021]

Europe Insurance (2022). Economic institutions and individual ethics: A study of consumer attitudes toward insurance fraud. 32(2), pp.247-265.

European Commission. (2017). Communication from the Commission to the European Parliament, The European Economic and Social. EU Strategy to Tackle Organised Crime pp.2021-2025. Brussels.

Fagerberg, J. (2008). *Occupational Fraud: Auditor's Perceptions of Red Flags and Internal Control: Linking Studies in Science and Technology* Thesis No 1369.

Federal Bureau of Investigation (2018). Fraud and Counter Measures. FBI.

Federal Bureau of Investigation (2018). Crime in the United States of America. Criminal Justice Information Services Division.

Federal Bureau of Investigation. (2018). Insurance Fraud. Official Website of the United States Government. USA.

Finscope Survey (2014). Finscope Consumer Survey Zimbabwe 2014. RBZ Working Papers Series.

- First Mutual Holdings, (2015). Survey on on Fostering Rural Growth through Micro Insurance. *Global Management Review February* 4(2): pp.7-13.
- Fisbein, M. & Ajzen, I (1975) *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Reaserch*. Reading Ma: Addison-Wesley.
- Ford Foundation. (2000). 2000 Annual Report. Mexico.
- Frey, U.J. & Pirsche, F. (2019). Distinguishing Protest Responses in Contingent Valuation: A Conceptualization of Motivations and Attitudes Behind Them. *Plos One*, 14(1), Pp. 1 -20
- Friedman, L. M. (1953). *American Law in the 20th Century*, New Haven: Yale University Press.
- Frimpong, I. (2016). *Causes, Effects and Deterrence of Insurance Fraud: Evidence from Ghana*. University of Ghana. (Mphil- Thesis).
- Geneva Association. (2012). *The Social and Economic Value of Insurance*. A Geneva Association Paper on Insurance Economics. September 2012.
- Geneva Papers On Risk and Insurance (2004). *Social Issues on Micro Insurance*. 14(2), pp.1-30.
- Geneva Papers On Risk and Insurance (2004). *Issues and Practice* 40 (1), pp131-158.
- Geyer, H. (2016). Poverty Traps in South African Agriculture. *Agrekon*, 55(4), pp.356-376.
- Gliner A., Morgan, G. & Leech, L. (2017) *Research Methods in Applied Settings: An Integrated Approach to Design and Analysis*, Second Edition 2nd Edition.
- Gliner, J.A., Morgan, G.A. & Leech, N.L. (2017). *Research Methods in Applied Settings: An Integrated Approach to Design and Analysis*. 3rd Edition. New York, Ny: Routledge.
- Global Study on Occupational Fraud and Abuse (2020). The control of insurance fraud a comparative view. *British Journal of Criminology*, 30(1), pp.1-23.
- Gogtay, N.J. & Thatte, U.M. (2017). Principles of Correlation Analysis. *Journal of the Association of Physicians of India*, 65(3), pp.78 – 81.
- Goodman, M.A. (2000) *Espionage and Covert Action*. In C. Eisendrath (Ed.) *National Insecurity: U.S. Intelligence After the Cold War*. Philadelphia: Temple University Press
- Gordon, L (2021). The institutionalization of deceptive sales in life insurance: Five sources of moral risk. *British Journal of Criminology*, 46, 993–1010.
- Grace, J.B. & Bollen, K.A. (2005). Interpreting The Results from Multiple Regression and Structural Equation Models. *The Bulletin of the Ecological Society of America*, 86(4), pp.283-295.

- Gray, D.E. (2014). *Doing Research in the Business World*. London: Sage Publication Ltd.
- Greene, R. (2021). Historical Development of Insurance. *Encyclopedia Britannica*. Sky Valley, Ga.
- Hair, J. F., Gabriel, M. & Patel, V. (2014). Amos Covariance-Based Structural Equation Modeling (Cb-Sem): Guidelines On Its Application as A Marketing Research Tool. *Brazilian Journal of Marketing*, 13(2), pp. 44 – 55.
- Hair, J.F., Risher, J.J., Sarstedt, M. & Ringle, C.M. (2019). When to Use and How to Report the Results of Pls-Sem. *European Business Review*, 31(1), Pp. 2 – 24.
- Hall, D. (2020). Contingent Valuation: Past, Present and Future. *Prague Economic Paper*, University of Economics, Prague, 2010(4), pp.329 - 343.
- Hart, T. (2011). *Inequalities in agricultural support for women in South Africa*. Policy brief. Pretoria: Human Sciences Research Council of South Africa.
- Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural Equation Modeling: Guidelines for Determining Model Fit. *The Electronic Journal of Business Research Methods*, 6, pp.53-60.
- Hooper, G. (2010). Investigating fraud in Insurance Industry. Intelligence techniques. *Economic Intelligence Survey*, Zimbabwe.
- Hooper, J. (2010). Effects of Fraud Control Mechanism on the Growth of Insurance Companies in Zimbabwe *Journal of Innovative Social & Science Education Research*, 2(1), pp26-39.
- Hox, J.J. & Bechger, T.M. (1998). An Introduction to Structural Equation Modeling. *Family Science Review*, 11, pp. 354 – 373.
- IAIS (2007), Report on the Survey on Preventing, Detecting and Remediating Fraud in Insurance, International Association of Insurance Supervisors, Basel.
- In'nami, Y. & Koizumi, R. (2013). Structural Equation Modeling in Educational Research: A Primer. In: M.S. Khine (Ed.). *Application of Structural Equation Modeling in Educational Research and Practice. Contemporary Approaches to Research in Learning Innovations*. Rotterdam: Sense Publishers.
- President's Department (2012). "KGB Foreign Intelligence from Brezhnev to the Coup." *Intelligence and National Security* 8, no. 3 (1993): pp52–67.
- Institute for Security Studies, (2018). *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*. New York: HarperCollins Publishers, 1990.

Institute Of Chartered Accountants In England And Wales (2020). Doing a Business in 2020. Audit and Assurance Faculty.

Institute of Internal Finance, (2016). IMF Annual Report 2016. Finding Solution Together

Insurance Act Chapter 24:07. (2004). Published in the Government of Zimbabwe Gazette (109) Harare Government Printers.

Nduna (2020). Insurability in Micro Insurance Markets: An Analysis of Problems and Potential Solutions. Geneva Papers on Risk & Insurance - Issues & Practice 37(1): pp77-107.

Insurance and Pension Commission. (2020). Reducing vulnerability: demand for and supply of micro insurance in Zimbabwe 17(3): pp.319-325.

Insurance and Pensions Commission (2017). Insurance Fraud and the form Zimbabwe Dollar to the United States Dollar Period.

Insurance Association of Zimbabwe (2021). Participation in Micro Life Insurance and the Use of Other Financial Services in Zimbabwe. Report 78(1): pp.7-35.

Insurance Europe (2018). Annual Report 2018/2019. Europe

Insurance Europe (2019). Annual Report 2019/2020. Europe

Insurance Europe. 2022. Annual Report 2020. Europe.

Insurance Fraud in the Digital Age, (2017). Business and Technology Trends: Defined Contribution Retirement Plans. Interactive Media.

Insurance Information Institute (2022). A Survey of Micro Insurance Companies in Zimbabwe. Unpublished Project, University of Zimbabwe. Harare.

Insurance Information Institute. (2018). The Insurance Handbook. A Guide to Insurance: What It Does and How It Works. New York

International Association of Insurance Supervisors (2007). Issues in Regulation and Supervision of Microinsurance. Basel, Switzerland.

International Association of Insurance Supervisors (2007). Issues Paper on Corporate Governance.

International Association of Insurance Supervisors (2008). Issues in regulation and supervision of microinsurance. Basel.

International Association of Insurance Supervisors. (2017). Annual Conference. Kuala Lumpur, Malaysia

International Labour Organisation (2006) Global Conference on Insurance and Reinsurance for Natural Catastrophe Risks (2006). Istanbul, December 8-9, 2005.

International Labour Organisation (2009). World Work Report 2009.

International Labour Organisation (2010). World Work Report 2009.

International Labour Organisation (2017). The Role of Micro Insurance as A Tool to Face Risks in The Context of Social Protection. [Internet:: [Http://Www. Ilo.Org/ Wcmsp5/ Groups/Public/---Ed_Protect/ Soc_Sec/ Documents/ Instructionalmaterial/ Wcms_Secsoc_93. Pdf](http://www.ilo.org/Wcmsp5/Groups/Public/---Ed_Protect/Soc_Sec/Documents/Instructionalmaterial/Wcms_Secsoc_93.Pdf); Downloaded On 2 September 2022.]

International Organisation for Migration (2019). International Migration 2019 Report. Department of Economic and Social Affairs.

Interpol, (2018). Annual Report 2018.

Jehanzeb K & Bashir N (2013). Training and Development Program and Its Benefits to Employee and Organization: A Conceptual Study. *European Journal of Business And Management*. (5).2.

Jeffery, C. R. (1977). Crime Prevention through Environmental Design (Second ed.). Beverly Hills, CA.: Sage.

John, C. (2014). Zimbabwe Rural-urban relations, household income diversification and agricultural productivity. *Development and Change* 22, pp.519-45.

Joint Operations Command on Peace and Securityt. (2020). Seminar on Mozambique Conflict

Josephine, S. John, B. I. Dingani, M. Nadine, S. Stephan, B & Antony, M. (2021). Hazards And

Jung & Jik-Kim, (2021). Insurance Fraud In Korea, Its Seriousness, And Policy Implications. [Internet [Https://Doi.Org/10.3389/Fpubh.2021.791820](https://doi.org/10.3389/fpubh.2021.791820)] Downloaded On 20 August 2020

Kanengoni, P. (2020). Issues in Regulation and Supervision of Micro insurance. Harare, Zimbabwe.

Karim, S. (2014) Job Satisfaction of Employees in Banking Sector: A Case Study On Janata Bank Limited. *International Journal of Evaluation and Research in Education*, 3, pp.152-157.

Karonga (2013) Dishonesty in everyday life of policy holder in Zimbabwe and its policy implications.25(1), pp117–126.

Kassem R. (2014). Detecting Asset Misappropriation: A Framework for External Auditors. *International Journal of Accounting, Auditing and Performance Evaluation* 10(1), pp1-42.

Kassem, S. (2014). Implementing Total Quality Management in Education: Compatibility and Challenges. *Open Journal of Social Sciences*, 4, pp.207-217.

Kassem, L. (2014). Detecting Asset Misappropriation: A Framework for External Auditors. [Internet [Http://Www.Inderscience.Com/Info/Inarticle.Php?Artid=59181](http://Www.Inderscience.Com/Info/Inarticle.Php?Artid=59181) downloaded On 10 July 2021]

Kestin, S, O'matz, M, & Maines, J. (2014). Organized Crime In Insurance Fraud: An Empirical Analysis of Staged Automobile Accident Rings.

Kelly, P. and Hartley, C. A. (2010). Casino gambling and workplace fraud. A cautionary tale for managers. *Management Research Review*, Vol. 33, No. 3, pp.224-239.

Kleemans, E. (2012). Organized Crime and The Visible Hand: A Theoretical Critique On the Economic Analysis of Organized Crime Syndicates. *Criminology & Criminal Justice* 13(5) pp615–629.

KPMG (2013). Fraud cases in Africa. [Internet: <http://newsghana.com.gh/fraud-cases-in-africa-reach-10-8b-in-2011-kpmg/> Downloaded on 3 March 2022]

KPMG International (2016). Global Profiles of the Fraudster: Technology Enables and Weak Controls Fuel the Fraud.

KPMG Zimbabwe (2021). Tax Highlights 2021 National Budget Statement. Harare.

KPMG. (2017). Closing The Gap. Cyber Security and the Insurance Sector. Kpmg Uk.

KPMG. (2020). Who is the typical fraudster? KPMG International, Switzerland.

KPMG. (2021). The South African Insurance Industry Survey 2021. South Africa

Labour and Economic Development Research Institute of Zimbabwe. (2019). Policy Brief on The 2018/2019 Labour Issues. Harare: Department of Labour.

Larkin, I & Leider, L. (2012). Incentive Schemes, Sorting, And Behavioral Biases of Employees: Experimental Evidence. *American Economic Journal of Microeconomics* (4)2, pp.184-214

Lesch, W., & Byars, B. (2008). Consumer insurance fraud in the US property-casualty industry. *Journal of Financial Crime*, 15(4), pp. 411–431.

Lester., (2009). Toward an industry campaign strategy on consumer insurance fraud, Presentation at Coalition against Insurance Fraud-Insurers' Roundtable Conference, Washington, DC 2005.

- Lister, L., M. (2007) 'A Practical Approach to Fraud Risk: Comprehensive Risk Assessments Can Enable Auditors to Focus Antifraud Efforts on Areas Where Their Organization is Most Vulnerable' *Internal Auditor* 64(6) 61-66
- Levi, M. (2008). Measuring the Impact of Fraud in the UK A Conceptual and Empirical Journey. *British Journal of Criminology*, 48(3), pp.293-318.
- Levi, M., & Burrows, J. (2008). Measuring The Impact of Fraud in The Uk a Conceptual and Empirical Journey. *British Journal of Criminology*, 48(3) pp 293-318.
- Liang, H. and Xue, Y. (2010) Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 11, 394-413.
- Likert, R. A. (1952). A Technique for The Development of Attitude Scales. *Archives of Psychology, Journal* 12(2) pp313-5.
- Lincoln, Y. S., & Guba, E. G. (2000). Paradigmatic Controversies, Contradictions, and Emerging Confluences. In N. K. Denzin, & Y. S. Lincoln (Eds.), *The Handbook of Qualitative Research* (2nd Ed., Pp. 1065-1122), Thousand Oaks, Ca: Sage Publications.
- Lister, M. (2007). Institutions, Inequality and Social Norms: Explaining Variations in Participation. *The British Journal of Politics and International Relations*, 9(1), 20–35.
- Lloyds. (2009). Insurance in Developing Countries: Exploring Opportunities in Micro Insurance.
- Loewe, M., Beblon, Y. (2009): The potential of microinsurance for social protection: *Journal of Insurance and Risk Management* 4 (1), 72-90.
- Longbottom, D. & Lawson, A. (2019). Alternative Research Methods: Introducing Market Sensing—A Qualitative and Interpretive Perspective On Research. In: P.M.W. Hackett (Ed.). *Quantitative Research Methods in Consumer Psychology: Contemporary and Data-Driven Approaches*. New York, Ny: Routledge.
- López-Mosquera, N., García, T. & Barrena, R. (2014). An Extension of the Theory of Planned Behavior to Predict Willingness to Pay for The Conservation of an Urban Park. *Journal of Environmental Management*, 135(2014), pp. 91 - 99.
- Machijika, M. (2018). Insurance Regulation in Zimbabwe: Is It an Enabler or A Burden to The Sector. Harare, Zimbabwe.
- Machinjika (2018). Service-dominant logic: Reactions, reflections and refinements. *Marketing Theory*, 6(3), pp. 281–288.
- Magoronga, M. (2020). Fraudulent Claims Upset Insurance, Pensions Sectors. *Chronicle*. 25 August.

- Malgwi, R. (2006). Internal Controls for The Small Business: Skimming and The Fraud Triangle. *Internal Auditing* 20 (1), Pp.3 – 10.
- Matanga, T. (2018). Criminal Investigation Department 2018 Annual Report. Zimbabwe Republic Police Harare.
- Maslow, Abraham Harold. (1943) "A Theory of Human Motivation." *Psychological Review* 50.4: 370-396. [Internet: <http://psycnet.apa.org/record/1943-03751-001>. Downloaded on 5 June 2022]
- Mccord, M., & Roth., J. (2006). Insurance provision in the world's 100 poorest countries. Appleton, WI USA, Microinsurance Centre.
- Matul, Michal., Michael J. McCord, Caroline. Phily, and Job. Harms. 2009. "The Landscape of Microinsurance in Africa." In *The Landscape of Microinsurance in Africa*.
- Merry, A. Prashad, P. & Hoffarth, T. (2014). "Micro Insurance Distribution Channels Insights for Insurers," ILO Working Papers 995186991702676, International Labour Organization.
- Micro Insurance Network (2018). Annual Report. Europe
- Micro Insurance Network. (2013). Annual Report. Europe.
- Micro Insurance Network. (2020). The State of Micro Insurance. The Insider's Guide to Understanding the Sector. Luxembourgish Government
- Military Intelligence Six. (2017). Intelligence Briefing on Organised Crime and Fraud in Zimbabwe. Harare.
- Miner, (1980). Theories of Organizational Behavior. Dryden Press
- Minister of Finance and Economic Development Ncube (2020). National Policy on Fraud and Corruption. 3rd Draft, June 2004. Harare.
- Ministry of Home Affairs, (2017). The Security and Intelligence Foundation
- Ministry of Industry and Commerce (2020). 2020 National Budget. Harare: Parliament of Zibabwe
- Ministry of Justice and Paliamtrat Affairt (2019). Conference on legislation and Insurance Fraud 2019. Procceddings of the MJLPA conference on legislation and insurance fraud. Zimbabwe. Harare.
- Ministry of State Security, Zimbabwe (2020). *Covert Action as a Tool Counter Organised Crime in Zimbabwe*. Harare.
- Miyazaki, S. J. (2009). Technologies of Perception. Miyazaki in Theory and Practice. *Animation*, 4(1), pp 55–75.

- Mohajan, H.K. (2017). Two Criteria for Good Measurements in Research: Validity and Reliability. *Annals of Spiru Haret University*. Economic Series, 17(3), Pp.1 - 31.
- Money Laundering and Proceeds of Crime Act [Chapter 9:24]. (2013). Published in The Government Gazette, Zwe-2013-G-14274. Harare: Government Printers.
- Mounaji, I. (2020). Micro Insurance Sector: An Overview of the Market Development and Distribution Strategies in Africa. Dubai.
- Moyo, I. (2019). Emerging Threats in Zimbabwe. Seminar On Threats Assessment. President's Department. 1 March. Bulawayo.
- Mpofu, R.T. (2015). Dollarization and Economic Development in Zimbabwe: An Interrupted Time-Series Analysis. [Internet: <https://doi.org/10.22495/Rgcv5i4art4>. Pdf; Downloaded On 19 August 2021]
- Muchemwa, F. (2020). Personal Interview with Frank Muchemwa, Former Commissioner at The Zimbabwe Anti-Corruption Commission. 10 November. Harare.
- Mugari, I. & Obioha, E. (2018). Patterns, Costs, and Implications of Police Abuse to Citizens' Rights in The Republic of Zimbabwe. *Social Sciences*, 2018, Vol. 7(7) pp.1-14.
- Mullins, C. R. (2009). Effects of alfalfa hay inclusion rate on productivity of lactating dairy cattle fed wet corn gluten feed-based diets. *J. Dairy Sci.*, 92 (7): pp 3510-3516
- Muradzikwa, G. (2021). Insurance and Pension Commission.Consumer. *Education Newsletter*.6th Edition.11 November.
- Muradzikwa, G. (2022). Anti-Money Laundering and Combating the Financing of Terrorism Obligations for Regulated Entities Training. Insurance and Pension Commission 20-25 January. Harare.
- Murdock, H. (2008). "The three dimensions of fraud". Internal Auditor, pp.1-14.
- .Musonza (2018), Micro Insurance and Low Income Earners in Zimbabwe.
- Mutual, M. Mccord, M. Phily, C. & Harms, J. (2009). The Landscape of Micro Insurance in Africa. Micro Insurance Innovation Facility. International Labour Organization.
- Mwanza W. (2014). An Analysis of Main Forces of Workplace Fraud in Zimbabwean Organizations: The Fraud Triangle Perspective. *SSNR Electronic Journal* 3(2): pp86-94.
- Nardi, P.M. (2016). Doing Survey Research: A Guide to Quantitative Methods. 3rd Edition. New York: Routledge.
- National Association of Insurance Commissioners of United States. (2019). International Insurance Forum Wraps. Washington, D.C.

National Social Security Act Chapter 17:04 (1989). Published in The Government Gazette, Zve-1989-L-29274. Harare: Government Printers.

National Social Security Authority (2021). The Role of Micro Insurance as a Tool to Face Risks in the Context of Social Protection. [Internet::http://www.ilo.org/wcmsp5/groups/public/ed_protect/soc_sec/documents/instructionalmaterial/wcms_secsec_93.pdf; downloaded on 25 February 2021.]

Naveh E, Meinch O & Marcus A. (2006). The Effects of Administrative Innovation Implementation On Performance. An Organizational Learning Approach. *Strategic Organization* 4(3): pp275-302.

Ncube, M. (2021). Personal Interview with Professor Mtuli Ncube Zimbabwe Minister of Finance and Economic Development. 10 May. Harare.

Neuman, W.L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*. 7th Edition. Essex: Pearson Education Limited.

Newton, L., Hayday, S. & Bekwaort, T. (2005). *Employee Assistance Programs*. Institute for Employment Studies.

Nwokocha, I. (2005). Managing Reward Strategy to Enhance Employee Performance, Retention and Productivity in Organizations: A General Overview. *International Journal of Development and Management Review* 1(11).

Nyoni, S. (2021). Keynote Address at A Ministry Strategic Planning Workshop. Kadoma. 18 October.

Okoth, J.R.A. (2014). *The Crime of Conspiracy in International Criminal Law*. Springer.

O'leary, P. (2014). *An Introduction to Document Analysis*. New York: Routledge.

Outreville. (2014). *The Essential Guide to Doing Your Research Project* (2nd Ed.). Thousand Oaks, CA: Sage Publications, Inc.

Park, S. & Lemaire, J. (2012). The impact of culture on the demand for non-life insurance. *ASTIN Bulletin: The Journal of the IAA*, 42 (2), pp. 501-527.

Peters, J. (2006). Perception of Influence in Insurance Fraud. *Journal of Criminal Law and Criminology*. (98)2, Pp. 363-427

Pew Research Center Survey (2017). Internet Connectivity Seen as Having Positive Impact On Life in Sub-Saharan Africa. Yasuyoshi Chiba.

Philip, P. (2013). *Security and Loss Prevention: An Introduction* (Sixth Edition). London.

President's Department (2017). Non Traditional Threats and Economic Development. Paper presented at the third conference on Non Traditional Threats in Zimbabwe. 8-17 October, Harare, Zimbabwe.

President's Department (2018). Training Manual on Surveillance. Operational Training Manual

President's Department (2021), Traditional and Non-Traditional Threats. Classified Intelligence briefs. Harare.

President's Department, Economic Intelligence Training Manual (2018) The Emergence of a New Cyber Weapon and Its Implications. 1 (2012): pp.80–91.

President's Department. (2019). Intelligence Brief on Human Security and Government Social Nets (Classified). Bulawayo. 20 October.

Price, L. (2020). Covid-19 (Coronavirus): Panic Buying and Its Impact On Global Health Supply Chains.

Proctor, K. (2021). Background Checks: The Theories Behind the Process. Uk.

Public Service Commission. (2021). Annual Report on Government Incentives 2020/2021. Harare.

Public Service Commission. (2021). Symposium on Micro Insurance for Government Employee. 1 March 2021.

Quah, J. (2017). Anti-Corruption Agencies in Asia Pacific Countries: An Evaluation of Their Performance and Challenges. Singapore

Rahman, W., Shah, F.A. & Rasli, A. (2015). Use of Structural Equation Modeling In Social Science Research. *Canadian Centre of Science and Education*, 11(4), Pp. 371 – 377.

Raskolnikov, A. (2019). Deterrence Theory: Key Findings and Challenges. Columbia Law.

Reinsurance Group of America. (2017). Global Claims Fraud Survey 2016/2017. United States of America.

Rejda, G. (2009). Principles of Risk Management and Insurance. 12th Edition.

Reserve Bank of Zimbabwe, (2016). From Bullets to Megabytes.” *The Herald*, January 26, 2020.

Reserve Bank of Zimbabwe. (2018). Monetary Policy Statement, Harare, Zimbabwe.

Road Traffic Act Chapter 13:11 (2020). Published in The Government Gazette, (16725) Harare: Government Printers.

Robert Gabriel Mugabe School of Intelligence Training Manual, (2020). The New Reality of Cyber War and the Intelligence Cycle.

Roff, M. (2017). Advancing Human Security through Artificial Intelligence. International Security Department and US and the Americas Programme. USA.

- Rogowski, R. (1997). The Regulation of Employment Relations. *Work, Employment and Society*, 11(1), pp.153–165.
- Roberts., L (2019). Microinsurance and microtakaful: Strategies for poverty reduction towards sustainable development. *OIDA International Journal of Sustainable Development*, 6(1), pp.93-100
- Russia's Federal Security Service. (2019). Inter-Agency Intelligence Notes. Moscow.
- Sarre, R. and Fiedler, B.A. (1999). ‘Investigating and Preventing Fraud against Australian Businesses: Counting the Costs and Exploring the Strategies’, *Accounting Forum*, 23(3), pp.275-292.
- Sausser, W.I. (2007). *Fostering and Ethical Culture for Business: The Role of HR Managers. Contemporary Issues, Challenges and Opportunities*, Information Age Publishing, Charlotte, pp253-285.
- Schober, P., Boer, C. & Schwarte, L.A. (2018). Correlation Coefficients: Appropriate Use and Interpretation. *Anesthesia & Analgesia*. 126(5), pp. 1763 – 1768.
- Schrum, M.L., Johnson, M., Ghuy, M & Gombolay, M.C. (2020). Four Years In Review: Statistical Practices Of Likert Scales In Human-Robot Interaction Studies. In: *Acm/Ieee International Conference on Human-Robot Interaction (Hri '20)*. Cambridge, 23 – 26 March, 2020
- Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum. *International Journal of Communications, Network and System Sciences*, 10(3).
- Senthilnathan, S. (2019). Usefulness of Correlation Analysis. Available at SSR 3416918.
- Silvello, A. (2017). Major Opportunities in Micro Insurance. *Insurance through Leadership*.
- Simpson, S. & Koper, C. (1992). Detering Corporate Crime. *Criminology Volume: 30 (3)*, PP.347-396.
- Singh, A.S. & Masuku, M.B. (2014). Sampling Techniques & Determination of Sample Size in Applied Statistics Research: An Overview. *International Journal of Economics, Commerce and Management*, 2(11), Pp. 1 – 22.
- Sivano, A. (2017). *IOTand Connected Insurance. Reshaping the Health Insurance Industry. A Customer-Centric “From Cure to Care” Approach*. *European Alliance of Innovation*. (Mini-Dissertation).
- Stecher, M. D., & Rosse, J. G. (2007). Understanding Reactions to Workplace Injustice Through Process Theories of Motivation: A Teaching Module and Simulation. *Journal of Management Education*, 31(6), 777–796.

- Stya, O. (2012). Questionnaire Designing for A Survey. *Journal of Indian Orthodontic Society*. 2012;46
- Subramanian, R., Asmawi, M.Z., & Sadikun, A. (2008). *Business Research Methods*. 8th Edition. New Castle: South-Western College Pub.
- Taherdoost, H. (2016). Determining Sample Size; How to Calculate Survey Sample Size. *International Journal of Economics and Management Systems*, 2(1), Pp. 237 – 239.
- Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in A Research. *International Journal of Academic Research in Management*, 5(3), pp.28.
- Technology in Micro Insurance, (2019). How New Developments Affect the Work of Actuaries. Society of Actuaries.
- Texas A&M University (2012). Enrolment File. Thousand Oaks, CA: Sage Publications.
- The Central Intelligence Agency (1991). *The Secret History of the CIA, Afghanistan, and Bin Laden, From the Soviet Invasion to September 10, 2001*. New York: Penguin Books.
- The Chartered Institute of Management Accountants. (2008). *Fraud Risk Management a Guide to Good Practice*.
- The Chartered Institute of Public Finance and Accountancy. (2015). *Fraud and Corruption*
- The Coalition against Fraud (2020). *The State of Insurance Fraud Technology Study*. Washington, D.C. Coalition against Fraud. Group. New York, Ny: Routledge.
- The Criminal Procedure and Evidence Act Chapter (2016). Published in the Government Gazzette Vol. XCIV, No. 34. Harare: Government Printers
- The International Association of Insurance Managers (2017). 2017. Annual Conference. Kuala Lumpur, Malaysia.
- The Ministry of Small and Medium Enterprise Development (2019). Census on low income earners. Harare, Zimbabwe.
- The President's Department (2019) *Overcoming the threat of insurance fraud in Zimbabwe: An assessment of drivers, constraints and opportunities*. Harare. Zimbabwe.
- The Reserve Bank of Zimbabwe's (2019). *Impact of Current Legislation on Fraud and Corruption*. Financial Intelligence Units Paper presented at the National Security Symposium. 1 June, Inyanga. Zimbabwe.
- The Zimbabwe Republic Police (2022). *Trends and Issues in Crime and Criminal Justice*, PGHQ: Criminal Investigation Department. Harare.

- Triandis, H.C. (1980) *Values, Attitudes, and Interpersonal Behavior*. Nebraska Symposium on Motivation, University of Nebraska Press, Lincoln.
- Tseng, F. C., & Kuo, F. Y. (2014). A Study of Social Participation and Knowledge Sharing in the Teachers' *Online Professional Community of Practice*. *Computers & Education*, 72, 37-47.
- Turner, R. (2005) Management Challenges to Implementing Agile Processes in Traditional Development Organizations. *IEEE Software*, 22, pp 30-39.
- United National (1983). Universal Declaration of the Rights of Peoples. *Social Justice. Human Rights & Peoples' Rights: Views from North & South*. 1 (35) pp. 155-158
- United Nations Conference on Trade and Development (1994). Trade and Development Report. Geneva. UN.
- United Nations Convention against Transnational Organized Crime. (2003). Un General Assembly Resolutions Adopting The UNTO and Its Protocols. Geneva.
- United Nations Office on Drugs and Crime (2004). United Nations Convention against Transnational Organized Crime and the Protocols Thereto. Vienna: UNODC.
- United Nations Human Rights. (1966). General Assembly Resolution 2200a (Xxi). International Covenant On Economic, Social and Cultural Rights. UN.
- United Nations. (2017). Human Security Theory and Practice. Application of The Human Security Concept and The United Nations Trust Fund for Human Security. Geneva. UN.
- United States of America Association of Certified Fraud Examiners. (2020). Global Fraud Conference. Virtual Conference. 31st Acfe Annual Conference 22-24 June 2020
- Vaughan, E. (1997). Risk Management Theory: The Integrated Perspective and Its Application in The Public Sector. *Estado, Gobierno, Gestión Pública*. pp 89-126.
- Vaughan, J. (1997). Risk Management. USA: John Wiley & Sons.
- Verma, R. Mani, S. (2019). Using Analytics for Insurance Fraud Detection. A New Opportunity for Fraud Detection. USA.
- Viane, S & Dedene, G. (2004). Insurance Fraud: Issues and Challenges. *Palgrave Macmillan Journals*. 29(2): pp. 313-333.
- Viscusi, W. Vernon, J. & Joseph E. Harrington, J. (2000). *Economics of Regulation and Antitrust*. 4th Ed. Broadway, Cambridge.
- Vishwakarma, G. (2017). Sample Size and Power Calculation. In: *Research Methodology*, Chapter: Sample Size and Power Calculation, (Pp.1 - 21).

- Vogt, W. P. (1999). *Dictionary of Statistics and Methodology: A Non-Technical Guide for the Social Sciences* (2nd Ed.). London: Sage Publications.
- Vogt, W. P., (1999). *Dictionary of Statistics and Methodology: A Non-Technical Guide for The Social Sciences* (2nd Ed.). London: Sage Publications.
- Von Lampe, K. (2016). *Organized Crime: Analysing Illegal Activities, Criminal Structures, and Extra-Legal Governance*.
- Vona, L. (2008). *Fraud Risk Assessment. Building a Fraud Audit Program*. Wiley.
- Walliman, N. (2011). *Research Methods: The Basics*. Abingdon: Routledge
- Walster, E., Walster, G. W., & Traupmann, J. (1978). Equity and premarital sex. *Journal of Personality and Social Psychology*, 36(1), pp.82–92.
- Walster, E., Walster, G. W., & Traupmann, J. (1978). Equity and premarital sex. *Journal of Personality and Social Psychology*, 36(1), pp.82–92.
- Wang, J. & Wang, X. (2020). *Structural Equation Modeling: Application Using Mplus*. 2nd Edition. Oxford: John Wiley & Sons.
- Weisbur, D. (1995) Crime Places in Crime Theory. In: Eck, J.E. and Weisburd, D., Eds., *Crime and Place, Crime Prevention Studies*, Vol. 4, Willow Tree Press.
- Westland, J.C. (2015). *Structural Equation Models: From Path to Networks*. Studies in Systems, Decision and Control, 22. New York, Ny: Springer.
- Wilson, G. (2004). Online interaction impacts on learning: Teaching the teachers to teach online. *Australasian journal of educational technology*, 20(1) pp. 3-28.
- Watts, S. & McDermott, V. (2015) Why would I hang around with you? The psychology of personal relationships, in Capdevila, R., Dixon, J. & Briggs, G. (Eds). *Investigating Psychology 2 - From social to cognitive*, Milton Keynes: The Open University.
- Wolfe, D., & Hermanson, D. R. (2004). The Fraud Diamond: Considering Four Elements of Fraud. *The CPA Journal*, 74, pp38-42.
- World Bank (2020). *2020 Annual Report on Zimbabwe*. Harare.
- World Bank. (2018). *Overcoming poverty and inequality in South Africa: An assessment of drivers, constraints and opportunities*. Washington, D.C.: World Bank Group.
- World Bank. (2020). *Financial protection against natural disasters: an operational framework for disaster risk financing and insurance*. Washington, DC.: World Bank Group.
- World Bank. (2020). *Zimbabwe Economic Update*. [Internet: <https://www.worldbank.org/en/country/zimbabwe/overview>] Downloaded On 4 July 2021

World Bank. (2020). Zimbabwe Overview. Development News, Research and Data. [Internet <https://www.worldbank.org/en/country/zimbabwe/overview#1> Downloaded On 15 July 2021].

World Health Organisation. Regional Office for Africa. (2020). Covid-19 News Letter. Geneva.

Wright, P. (2010). Recent initiatives in the prevention and detection of insurance fraud in Zimbabwe. *Journal of Financial Crime*, 4 (3), pp.236-241

Yore, R. & Walker, J.F. (2019). Micro Insurance for Disaster Recovery: Business Venture or Humanitarian Intervention? An Analysis of Potential Success and Failure Factors of Micro Insurance Case Studies. *International Journal of Disaster Risk Reduction*, Pp. 16 – 32.

Yu, T.W. & Chen, M.S. (2014), "Developing Life Insurer-Insurance Intermediary Relationships", *Managing Service Quality: An International Journal*, 24(5) pp. 455-468.

Yusuf, O. T., & Babalola, A. R. (2009). Control of insurance fraud in Nigeria: an exploratory study (case study), *Journal of Financial Crime*, 16 (4), pp418-435.

Yusuf, S.M (2010) TQM Implementation Issue: Review and Case Study. *International Journal of Operation and Production Management*, 20, pp.634-655.

Zhong, M., Sun, Z., Lai, G. & Yu, T. (2015). Cultural influence on insurance consumption: Insights from the Chinese insurance market. *China Journal of Accounting Studies*, 3(1), pp. 24 – 48.

Ziegler, M. & Hagemann, D. (2015). Testing The Unidimensionality of Items: Pitfalls and Loopholes. *European Journal of Psychological Assessment*, 31(4), pp. 231 – 237.

Zimbabwe Anti- Corruption Commission, (2020). Economic Governance Watch 02/2020. ZACC Powers.

Zimbabwe Economic Forum (2019). Moral, Social, and Economic Dimensions of Insurance Claims Fraud. *Journal of Social Research* 75(4): pp.1181-1204.

Zimbabwe Insurance Association (2018) Insurance in Developing Countries: Exploring Opportunities in Micro insurance.

Zimbabwe Intelligence Community (2021). Intelligence brief on organised crime and insurance fraud. Harare: Joint Operations Command.

Zimbabwe Intelligence Community. (2021). Human Security Classified Intelligence Brief. 20 April. Harare.

Zimbabwe Joint Operations Command (2019). Interagency Intelligence on Organise Crime Operations. Report Presented to the Sub-National JOC on Security. 7 November. Harare: Zimbabwe.

Zimbabwe Ministry of Finance and Economic Development (2020). Low Income Eaners Resilience Initiative - Quarterly report - January - March 2020.

Zimbabwe National Statistics Agency (2020). 2020 Population Census Report. Harare

Zimbabwe National Statistics Agency (2021). Labour Force and income Census Report 2020/2021. Harare.

Zimbabwe National Statistics Agency. (2021). National Employment Demographics. Harare. Government Printers.

Zimbabwe Republic Police (2019). Integrative Service Delivery ZRP Outpost. Harare, Government Printers.

Zimbabwe Republic Police, Criminal Investigations Department (2020). Criminal Docket on Insurance Fraud. CID Head Quarters.

Zimbabwe Statistics Agency (2020). Lowincome Workforce Census. Harare. Department of Lobour

Zimbabwe Surveyor General (2020). Brief on 2022 Delimitation Exercise. Harare: Mapping and Research.

Zimbabwe's National Statistical Agency (2021). 2021/2021 Labour Census. Bulaywa: Compensation House.

Zimbabwe's National Statistical Office (2021). Low Income Household Census 2021 Report. Harare

Zimbabwean Intelligence Community (2018). Low Income Household Census 2018 Report. Harare.

Zimmerman, Et Al., (2013). Constructing the insurance relationship: Sales stories, claims stories, and insurance contract damages. *Texas Law Review*, 72, pp.1395–1443.

Zinyama, C. (2010). Systemic Corruption in Zimbabwe. University of Zimbabwe Press.

Zinyama, T. (2010). Systemic Corruption In Zimbabwe: Is The Human Factor The Missing Link? African Journal of Public Affairs. *Sabinet African Journal of Public Affairs* 12 (1).

APPENDICES

Appendix A: Informed Consent Form.



GRADUATE SCHOOL OF BUSINESS AND LEADERSHIP

Consent Letter

Participant

RE: INVITATION TO PARTICIPATE IN A RESEARCH PROJECT

Reference is made to the above.

My name is Soul Nyangoni, a Doctor of Business Administration (DBA) student at the University of KwaZulu Natal. I kindly invite you to participate in a research project entitled: DEVELOPING AN INTELLIGENCE AND SECURITY FRAMEWORK TO COUNTERACT INSURANCE FRAUD IN THE LOW INCOME SECTOR. THE CASE OF ZIMBABWE. The objective of this study is to profile practical insurance fraud counter measures.

Your participation in this study will go a long way in defining the current nature of insurance fraud, how it is linked to organised crime syndicates, why is it targeting service providers offering services to low income earners, socio-economic impact of insurance fraud and how a national intelligence and security agency or organisation can assist in detecting and countering insurance fraud. Findings of this research are expected to contribute towards the integration of the insurance industry and state security in countering insurance fraud. The survey should take you between ten (10) and fifteen (15) minutes and participation is voluntary with an option to withdraw from the project.

To note is that the research requires disclosure of classified information, the researcher and the UKZN, Graduate School of Business and Leadership assures to maintain the highest level of confidentiality of information provided and identity protection of participants.

For clarity and further information, kindly contact the UKZN research office, the researcher or the supervisor on contact details below.

NO	POSITION	NAME	PHONE	EMAIL
1	RESEARCHER	MR. SOUL NYANGONI	+263 772 144 122	soulnyangoni@gmail.com
2	SUPERVISOR	DR BIBI ZAHEENAH CHUMMUN	+277 31 260 8943	chummunb@ukzn.ac.za
3	RESEARCH OFFICE	HSSREC RESEARCH OFFICE	Tel: 031 260 8350/4557/3587	<u>hssrec@ukzn.ac.za</u>

Your participation in this research will be greatly appreciated.

Yours faithfully



Soul Nyangoni

Researcher: Doctor of Business Administration (DBA)

University of KwaZulu Natal

Researcher's Copy

CONSENT FORM

I..... (full names of the participant)
..... (Name of organisation or company/ Policy holder)
have been informed about the study entitled DEVELOPING AN INTELLIGENCE AND SECURITY FRAMEWORK TO COUNTERACT INSURANCE FRAUD IN THE LOW INCOME SECTOR. THE CASE OF ZIMBABWE. I have been given an opportunity to answer questions about this study. I do hereby confirm that I voluntarily consent to participate in this research. Terms, conditions and the nature of this research have been explained to me. I have also read and understood this document. I fully understand that this is voluntary participation and I'm allowed to withdraw from the project in the event that I decide to do so.

If I have any further questions, concerns and or queries related to the study I understand that I may contact the researcher, supervisor and or the research office in which their contacts have already been provided to me.

Signature..... Date.....

Appendix B: Questionnaire

PART A

DEMOGRAPHIC INFORMATION

1. WHAT IS YOUR GENDER?

MALE		FEMALE		PREFER NOT TO SAY	
------	--	--------	--	-------------------	--

2. WHAT IS YOUR AGE

18-35		35-44		45-54		55-65		+65	
-------	--	-------	--	-------	--	-------	--	-----	--

3. WHAT IS YOUR ETHNIC GROUP?

BLACK AFRICAN		COLOURED		WHITE		INDIAN/ASIAN		PREFER NOT TO SAY	
------------------	--	----------	--	-------	--	--------------	--	----------------------	--

4. WHAT IS YOUR MARITAL STATUES?

MARRIED		SINGLE		DIVORCED		WINDOWED		PREFER NOT TO SAY	
---------	--	--------	--	----------	--	----------	--	----------------------	--

5. WHAT IS YOUR HIGHEST LEVEL OF EDUCATION?

TERTIART		HIGH SCHOOL		SECONDARY		PRIMARY		PREFER NOT TO SAY	
----------	--	----------------	--	-----------	--	---------	--	----------------------	--

6. ARE YOU CURRENTLY EMPLOYED OR A POLICYHOLDER PUT AN X WERE APPLICABLE?

Insurance Company		Intelligence, Security Service		Policyholder	
-------------------	--	--------------------------------	--	--------------	--

7. If employed is your employment status

PERMANENT		PART TIME	
-----------	--	-----------	--

8. WHAT IS YOUR CURRENT POSITION IN THE COMPANY?

UPPER MGT		MIDDLE MGT		LOWER MGT		OTHERS	
-----------	--	------------	--	-----------	--	--------	--

9. FOR HOW LONG HAVE YOU BEEN EMPLOYED OR A POLICY HOLDER?

-5		5-10		11-15		16-20		+20	
----	--	------	--	-------	--	-------	--	-----	--

PART B
QUESTIONS FOR THE REGULATORY AUTHORITY

NO		1= Strongly Disagree: 2=Disagree: 3= Neutral: 4= Agree: 5= Strongly Agree				
		1	2	3	4	5
1	Insurance fraud is always initiated by someone who organizes individuals to assist in this act?	1	2	3	4	5
2	In your investigations, do employees and policy holders connive with organized crime syndicates?	1	2	3	4	5
3	Can intermediaries aid the crime of insurance fraud?	1	2	3	4	5
4	To what extent do you thing that former employees can aid insurance fraud?	1	2	3	4	5
5	Insurance fraud is highly targeted at low income earners or companies offering services to low income earners?	1	2	3	4	5

NO	IN YOUR OPINION, CAN THE FOLLOWING FACTORS LEADS TO ORGANISED INSURANCE FRAUD?	1= Strongly disagree: 2=Disagree: 3= Neutral: 4= Agree: 5= Strongly Agree				
		1	2	3	4	5
	Companies offering services to low incomes earners hardly invest in technologically to detect insurance fraud which creates opportunities for criminals?					
	Are internal controls effective in detecting insurance fraud?					
	Poor supervision of intermediaries' activities: Policyholder insured lives beyond the region were the broker or agent operates are possible opportunities for insurance fraud?					
	Request for payments and or via the broker or agent correspondence is a possible opportunity for insurance fraud?	1	2	3	4	5
	Appointment of intermediaries without proper vetting, security background check and criminal record clearance?	1	2	3	4	5
	Historical failure by the police to detect and counter insurance fraud entices criminals?	1	2	3	4	5
	Lack of training	1	2	3	4	5

	IN YOUR OPINION, INSURANCE FRAUD IS AN ORGANISED CRIME?					
	Insurance fraud is prevalent where there is a structured group of three or more people?	1	2	3	4	5
	Does the group exists for a period of time	1	2	3	4	5
	The group acts in concert with the aim of committing at least one serious crime	1	2	3	4	5
	ACCESS TO THE INSURANCE COMPANY AND INSURANCE FRAUD?					
	In your opinion access to systems of the insurance fraud is vital for this kind of crime?	1	2	3	4	5
	Is access to operating procedure is equally important?	1	2	3	4	5
	Information on the financial position is also important?	1	2	3	4	5
	SAFEY, CONCEALMENT AND INSURANCE FRAUD?					
	Lack of mechanisms to detect insurance fraud is an indication of preserved safety by criminals?	1	2	3	4	5
	Information provided to organized crime syndicates that there is no monitoring of their criminal activities by security forces aid criminal activities?	1	2	3	4	5
	There is concealment of identity of other parties?	1	2	3	4	5
	Concealment of intension to co commit insurance fraud also aids?	1	2	3	4	5
	ORGANISED CRIME SYNDICATES NEED TO JUSTIFY THEIR CRIMINAL CONDUCT BEFORE ACTION?					
	They think what they are doing is right?	1	2	3	4	5
	They commit the crime because they think that the same companies are defrauding the general public?	1	2	3	4	5
	They need the money to finance fellow comrades, criminals who are in need?	1	2	3	4	5
	PERSEIVED REWARD					
	Do organized crime syndicates commit insurance fraud because there is perceived financial gain?	1	2	3	4	5
	The money obtained can be used to finance other related crimes?	1	2	3	4	5
	TO WHAT EXTENT DO THESE MOTIVATE ORGANISED CRIME CYNDICATES?					
	Coercion/ Enticement (ie, people could be forced or enticed by their peers, family or superiors)?	1	2	3	4	5
	Using funds to purchase criminal commodities ie, drugs or firearms?	1	2	3	4	5
	Ideology (ie, doing it for their idea of the 'greater good', such as the case of terrorist organisations)?	1	2	3	4	5

	The pathological desire for crime?	1	2	3	4	5
	Greed and financial need?	1	2	3	4	5

	AREAS/QUESTIONS	YES	NO
1	Is the economy being affected by Insurance fraud?		
2	Are policy holders' mainly low income earners being negatively affected by insurance fraud?		
3	Do insurance companies report cases of insurance fraud to the regulatory authority?		
4	Are the same cases being reported to the police?		
5	Do you think that organized crime syndicates are perpetrating insurance fraud?		
6	In cases of arrests and convictions, do you think the legislation is sufficient enough to deter insurance fraud?		
7	As a regulatory body do you have a watch list of criminals or individuals who were once involved in insurance fraud?		
8	Do regulatory authorities recommend counter insurance fraud strategies to insurance companies?		
	Do you think that working with the national intelligence community would be helpful in countering insurance fraud?		

NO	QUESTION	COMMENT
1	What effect do you think that insurance fraud has to:	Policy Holder
		The Company
		Policy Holder

		Investor
2	From the cases you received, has sufficient evidence been collected to secure convictions and conclude the cases?	
3	Do you have laws, acts policies and regulations which inhibit insurance fraud? (If yes kindly list them)	
4	In what circumstance are the laws, acts, policies and regulations functioning to curb insurance fraud?	
10	Can you list the types of insurance fraud that are prevalent in Zimbabwe?	
12	Do you as the regulatory body offer trainings and awareness on insurance fraud to insurance companies?	
13	If yes, what are the components of the training manual?	
14	Is everyone employed in the insurance industry entitled to attend the training or it's for specific departments?	
15	How frequent are these trainings done in a year?	
16	Do you offer the trainings to intermediaries?	
17	Are the trainings offered for free	

	or at a cost?	
18	Do you document the cost the industry loses to insurance fraud? If YES, on average, how much is lost annually?	

PART C
QUESTIONS FOR POLICY HOLDERS

NO	AREAS/QUESTIONS	YES	NO
1	Have you ever been a victim of insurance fraud?		
2	Did the fraud affect your access to service?		
3	Did you report the case to your service provider?		
4	Was the case reported to the police?		
5	Was the case concluded?		
6	Was the person involved identified and prosecuted?		
	Do you think the crime was organized?		
7	Is there any intervention by the government to counter insurance fraud?		
8	Is there any measures being put in place by your service provider to counter insurance fraud?		
9	Do you think that the Government has a role to play or a responsibility to counter insurance fraud		

Risk Preference

Please indicate to what extent you agree or disagree with the following statements:

	Strongly agree	Agree	Neutral	disagree	Strongly disagree
1 - Insurance culture					
I have a good understanding of how micro insurance works.					
I have considered using micro insurance to protect my assets and livelihood.					
I understand that paying for insurance does not guarantee a claim pay out.					

2 - Financial capability					
I have access to emergency savings for my small business operations and family.					
I have sufficient funds to do my operations for the next year.					
I manage my income and expenditure according to a planned budget.					
What kind of insurance services are you receiving?					
Which company is offering you the services?					

PART D
QUESTIONS FOR INSURANCE COMPANIES

NO		1= Strongly Disagree: 2=Disagree: 3= Neutral: 4= Agree: 5= Strongly Agree				
		1	2	3	4	5
1	Insurance fraud is always initiated by someone who organizes individuals to assist in this act?	1	2	3	4	5
2	Are managers involved in insurance fraud?	1	2	3	4	5
3	Do you think employees connive with organized crime syndicates?	1	2	3	4	5
4	Do you think policy holders connive with organized crime syndicates?	1	2	3	4	5
5	Can intermediaries aid the crime of insurance fraud?	1	2	3	4	5
	To what extent do you think that former employees can aid insurance fraud?					
6	Insurance fraud is highly targeted at low income earners or companies offering services to low income earners?	1	2	3	4	5
		1	2	3	4	5

NO	IN YOUR OPINION, CAN THE FOLLOWING FACTORS LEADS TO ORGANISED INSURANCE FRAUD?	1= Strongly disagree: 2=Disagree: 3= Neutral: 4= Agree: 5= Strongly Agree				
		1	2	3	4	5
		1	2	3	4	5

7	An opportunity for insurance fraud and related crimes exist in companies offering services to low income earners?					
8	Are internal controls effective in detecting insurance fraud?					
9	Companies offering services to low incomes earners hardly invest in technologically to detect insurance fraud?					
10	Poor supervision of intermediaries' activities: Policyholder insured lives beyond the region were the broker or agent operates are possible opportunities for insurance fraud?	1	2	3	4	5
11	Request for payments and or via the broker or agent correspondence is a possible opportunity for insurance fraud?	1	2	3	4	5
12	Appointment of intermediaries without proper vetting, security background check and criminal record clearance?	1	2	3	4	5
13	Historical failure by the police to detect and counter insurance fraud entices criminals?	1	2	3	4	5
14	Lack of training	1	2	3	4	5
	IN YOUR OPINION, INSURANCE FRAUD IS AN ORGANISED CRIME?					
15	Insurance fraud is prevalent where there is a structured group of three or more people?	1	2	3	4	5
16	Does the group exists for a period of time	1	2	3	4	5
17	The group acts in concert with the aim of committing at least one serious crime	1	2	3	4	5
	ACCESS TO THE INSURANCE COMPANY AND INSURANCE FRAUD?					
18	In your opinion access to systems of the insurance fraud is vital for this kind of crime?	1	2	3	4	5
19	Is access to operating procedure is equally important?	1	2	3	4	5
20	Information on the financial position is also important?	1	2	3	4	5
21						
	SAFEY, CONCEALMENT AND INSURANCE FRAUD?					
22	Lack of mechanisms to detect insurance fraud is an indication of preserved safety by criminals?	1	2	3	4	5
23	Information provided to organized crime syndicates that there is no monitoring of their criminal activities by security forces aid criminal activities?	1	2	3	4	5
24	There is concealment of identity of other parties?	1	2	3	4	5
25	Concealment of intension to co commit insurance fraud also aids?	1	2	3	4	5
	ORGANISED CRIME SYNDICATES NEED TO JUSTIFY THEIR CRIMINAL CONDUCT BEFORE ACTION?					
26	They think what they are doing is right?	1	2	3	4	5
27	They commit the crime because they think that the same	1	2	3	4	5

	companies are defrauding the general public?					
28	They need the money to finance fellow comrades, criminals who are in need?	1	2	3	4	5
	PERSEIVED REWARD					
29	Do organized crime syndicates commit insurance fraud because there is perceived financial gain?	1	2	3	4	5
30	The money obtained can be used to finance other related crimes?	1	2	3	4	5
	TO WHAT EXTENT DO THESE MOTIVATE ORGANISED CRIME CYNDICATES?					
31	Coercion/ Enticement (ie, people could be forced or enticed by their peers, family or superiors)?	1	2	3	4	5
32	Using funds to purchase criminal commodities ie, drugs or firearms?	1	2	3	4	5
33	Ideology (ie, doing it for their idea of the 'greater good', such as the case of terrorist organisations)?	1	2	3	4	5
34	The pathological desire for crime?	1	2	3	4	5
35	Greed and financial need?	1	2	3	4	5
	IN YOUR OPINION, ARE THESE MEASURES EFFECTIVE TO COUNTERINSURANCE FRAUD?					
36	Effective internal controls: establishment of clear responsibilities, elimination of the management of money flows by a single person, establishment of clear reporting lines and communication procedures.	1	2	3	4	5
37	Pre-employment initial vetting and security clearance and in-employment continuous vetting of management and staff especially those in claims units or department.	1	2	3	4	5
38	Pre-employment criminal clearance of management and staff especially those in claims units or department.	1	2	3	4	5
39	Clear legislation, acts and policy concerning fraud management by Zimbabwe Insurance and Pension Commission.	1	2	3	4	5
40	Product proofing (including fraud preventing characteristics when designing a product).	1	2	3	4	5
41	Emphasizing the consequences of fraud to the policyholder and claimant in the application form and in the contract.	1	2	3	4	5
42	Application of IT tools and techniques to check the authenticity of documents.	1	2	3	4	5
43	Adequate and routine training for independent brokers.	1	2	3	4	5
44	Assistance by the Government by giving the National Intelligence Organization the mandate to detect, investigate and counter insurance fraud.	1	2	3	4	5
45	Vetting, criminal record clearance and screening of the intermediaries to ascertain if they are fit to be licensed.	1	2	3	4	5
46	Vetting, criminal record clearance and screening of	1	2	3	4	5

	international clients.					
47	Sharing of notes and watch list between the two industries that is the intelligence and security and the insurance industry	1	2	3	4	5
NO	QUESTION	REMAERKS				
48	How is insurance fraud detected, is it via a technological aided system or a manual system?					
49	What procedure would be used to confirm the red flags as possible insurance fraud?					
50	Are you currently offering insurance services to middle managers and below in the following categories? (Indicate by a tick).					
		Civil Servants				
		Retail				
		Tourism				
		Mining				
		Informal Sector				
		Banking				
		Construction				
		Transport				
		Agriculture				
		Communication				
		Entertainment				
		Manufacturing				
		Security Guards				
		Processing				
51	At company level what measures are there to counter insurance fraud?					
52	Do you have a separate risk management unit or it the responsibility of the claims unit to investigate possible insurance fraud cases?					
53	Is your staff that is involved in detecting insurance fraud, collection of evidence and investigation cases has any specialized training in that regard?					
54	What are the specific					

	components of the training you offer to your staff?		
55	Is the training provided internal or externally?		
56	In your opinion, how effective are the trainings?		
57	When was the last time you had these trainings?		
58	Do you as an organization invest in technology to counter insurance fraud? If YES what type of technology?		
59	Do you hand over your cases of insurance fraud to the Zimbabwe Republic Police for further investigations?		
60	If YES, what is the success rate in percentage?		
61	Do you as an organization keep a watch list of criminals who are involved in insurance fraud?		
62	If YES, do you share the watch list at industry level or with either the ZRP or the National Intelligence Organization?		
63	What type of insurance fraud exists in your industry?		
63	Insurance fraud leads to increased operational costs on part of the insurance company?	YES	NO
64	Breach of insurance ethical standards?	YES	NO
65	Less revenue from Insurance Premium?	YES	NO
66	Bad reputation, locally and internationally?	YES	NO
67	Decline in market share?	YES	NO
68	Closure of insurance companies?	YES	NO
69	Increased funding of criminal activities?	YES	NO
70	Threat to national security and economic Development?	YES	NO

71	Do you have a dedicated department that focus on detecting insurance fraud?	YES	NO
72	Is this department involved in the investigation of fraud cases in conjunction with the police?	YES	NO
73	Are the current control systems in practice to detect insurance fraud and scams effective?	YES	NO
74	Does the suspects use any form of technology to conceal their insurance fraud activities or identity?	YES	NO
75	In your opinion, are investors willing to invest in the industry when insurance fraud is on the rise?	YES	NO
76	Is there any legislation currently available which deals with insurance fraud?	YES	NO
77	Is the legislation effective in countering insurance fraud?	YES	NO

PART E

QUESTIONS FOR INTELLIGENCE AND SECURITY COMMUNITY

SECRET

NO	AREAS/QUESTIONS	YES	NO
1	Do you consider insurance fraud a threat to national security?		
2	Is insurance an important component of human security?		
3	Is insurance fraud is highly perpetrated by organized crime syndicates?		
4	It is the responsibility of the Intelligence community to investigate and gather evidence with regards to insurance fraud?		
5	Does the National Intelligence Organization have a counter fraud or anti-corruption unit or department? If YES what is the role of this unit		
6	Does this unit have arresting powers?		
7	Is this unit cleared to work with other organizations or it works in isolation?		
8	Does the unit keep a watch list of criminals involved in fraud		
9	Does it share its notes with other organization?		
10	Apart from the human capital, is the unit technologically equipped to detect insurance fraud?		
11	Has your organization ever investigated and apprehended criminal wanted for insurance fraud related cases?		

NO	AREAS/QUESTIONS	REMARKS
12	What effect does fraud in general and insurance fraud in particular has to the country?	
13	What are the likely motives behind insurance fraud?	

14	In your opinion, why are these organized crime syndicates targeting insurance companies offering services to low income earner?	
15	Do you conduct both electronic and physical surveillance to criminals who were once involved in cases of insurance fraud?	
16	Apart from what has been stated what else do you do to counter insurance fraud?	
17	Do you think that the current legislation on insurance fraud is deterrent enough? If not what do you recommend?	
18	Do you as an organization offer specialized training on counter fraud to other organization?	
19	What other counter measures do you recommend?	

THANK YOU

Appendix C: Editorial Letter

HUMAN RESOURCES
RESEARCH CENTRE

Human Resources Research Centre
□ P.O. Box MP167, Mount Pleasant, Harare,
Zimbabwe
□ (263) 772241953
□ E-mail: gamatw@gmail.com



FACULTY OF EDUCATION

UNIVERSITY OF ZIMBABWE


14 June 2022

To whom it may concern

This serves to certify that the PhD document titled: *Developing an Intelligence and Security Framework to Counteract Insurance Fraud in the Low-Income Sector: The Case of Zimbabwe*, by **Soul Nyangoni**, was edited by an experienced editor/proofreader. I have edited the document and advised the author to effect various changes including the mechanics of language, formatting of text and referencing style.

I am of the view that the general quality of the document is of acceptable academic standards.

Thank you.


Thomas W. Gama
(Editor)

Appendix D: Gatekeeper Letter

Insurance & Pensions
Commission



21 September 2020

Soul Nyangoni
No. 4 Old Mutual Flats
Chiredzi

Dear Sir

AUTHORISATION TO CARRY OUT A PHD RESEARCH ON INSURANCE FRAUD

Reference is made to the above matter and to your letter dated 21 September 2020.


After considering your request, the Commission has no objection to you carrying out research on the topic *"Developing an intelligence and security framework to counteract insurance fraud in the low income sector. The case of Zimbabwe"* within the local insurance sector.

The Commission exhorts you to uphold all applicable legal and ethical requirements and standards in the conduct of your research.

We would be grateful if you could share with us the findings of your research as they may have a bearing on our regulatory activities.

We wish you success in your endeavours.

Yours Faithfully


G.Muradzikwa
Commissioner of Insurance, Pension and Provident Funds

Appendix E: Ethical Clearance



29 March 2021

Mr Soul Nyangoni (219015542)
Grad School Of Bus & Leadership
Westville Campus

Dear Mr Nyangoni,

Protocol reference number: HSSREC/00002507/2021

Project title: DEVELOPING AN INTELLIGENCE AND SECURITY FRAMEWORK TO COUNTERACT INSURANCE FRAUD IN THE LOW INCOME SECTOR. THE CASE OF ZIMBABWE.

Degree: PhD

Approval Notification – Expedited Application

This letter serves to notify you that your application received on 15 February 2021 in connection with the above, was reviewed by the Humanities and Social Sciences Research Ethics Committee (HSSREC) and the protocol has been granted **FULL APPROVAL**.

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number. **PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.**

This approval is valid until 29 March 2022.

To ensure uninterrupted approval of this study beyond the approval expiry date, a progress report must be submitted to the Research Office on the appropriate form 2 - 3 months before the expiry date. A close-out report to be submitted when study is finished.

All research conducted during the COVID-19 period must adhere to the national and UKZN guidelines.

HSSREC is registered with the South African National Research Ethics Council (REC-040414-040).

Yours sincerely,



Professor Dipane Hlalele (Chair)

/dd

Humanities and Social Sciences Research Ethics Committee

Postal Address: Private Bag X54001, Durban, 4000, South Africa

Telephone: +27 (0)31 260 8350/4557/3587 Email: hssrec@ukzn.ac.za Website: <http://research.ukzn.ac.za/Research-Ethics>

Founding Campuses:  Edgewood  Howard College  Medical School  Pietermaritzburg  Westville

INSPIRING GREATNESS