EFFECTIVENESS OF USE OF BIOMETRIC TECHNOLOGY TO CURB FRAUD IN MEDICAL INSURANCE FIRMS IN KENYA

BY

BARANABAS GISAIRO GISAIRO

D63/77937/2015

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTERS OF SCIENCE IN FINANCE, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI.

NOVEMBER, 2016

DECLARATION

Student's Declaration

This research project is my original work and has not been submitted to any other university or institution of higher learning for any academic award.

Signed…………………………………… Date …………………………………..

Baranabas Gisairo

Supervisor's Declaration

This research project has been submitted for examination with my approval as the university supervisor.

Signed…………………………………… Date …………………………………..

Dr. Mirie Mwangi

SENIOR LECTURER

UNIVERSITY OF NAIROBI

DEPARTMENT OF FINANCE AND ACCOUNTING

ACKNOWLEDGEMENT

I thank God Almighty for the ability and strength he has bestowed me with which has enabled me to complete this research project.

I wish to acknowledge the contribution of my colleague and mentor Benard Omwenga who encouraged me throughout the process of coming up with this research report.

I extend my appreciation to my supervisor, Dr. Mirie Mwangi for his guidance which provided me with necessary insight as I wrote and compiled this research report. I am also grateful to Dr. Kisaka Sifunjo for his guidance as my moderator

DEDICATION

This research project is dedicated to my parents Johnson Ondieki, Job Gisairo and Josephine Nyakerario and my brother Gerald.

Table of Contents

ACKNOWLEDGEMENT iii

DEDICATION iv

LIST OF TABLES vii

LIST OF ABBREVIATIONS viii

ABSTRACT ix

CHAPTER ONE 1

INTRODUCTION 1

1.1 Background of the study 1

1.1.1 Biometric Technology 2

1.1.2 Fraud in Insurance Industry 3

1.1.3 Biometric Technology and Fraud in Medical Insurance Firms 5

1.1.4 Medical Insurance Firms in Kenya 7

1.2 Research Problem 8

1.3 Objective of the Study 10

1.4 Value of the Study 10

CHAPTER TWO 11

LITERATURE REVIEW 11

2.1 Introduction 11

2.2 Theoretical Framework 11

2.2.1 Fraud Triangle Theory 11

2.2.2 The Fraud Diamond Theory 13

2.2.3 The Fraud Scale Theory 13

2.2.4 The Economic Contractual Theory 14

2.3 Determinants of Fraud in Medical Insurance Firms 14

2.3.1 Weak Internal Control Systems 15

2.3.2 Lack of Internal and External Audit Functions 15

2.3.3 Poor Corporate Governance Structures 16

2.4 Empirical Studies 17

2.5 Conceptual Model 21

2.6 Summary on Literature Review 22

CHAPTER THREE 23

RESEARCH METHODOLOGY 23
3.1 Introduction 23
3.2 Research Design 23
3.3 Population 24
3.4 Data Collection 24
3.5 Data Analysis 25
3.5.1 Analytical Model 25
3.5.2 Test for Significance 26
CHAPTER FOUR 27
DATA ANALYSIS RESULTS AND DISCUSSION 27
4.1 Introduction 27
4.2 Descriptive Statistics 27
4.3 Correlation Analysis 28
4.4 Regression Analysis 30
4.5 Discussion of Research Findings 32
CHAPTER FIVE 36
SUMMARY, CONCLUSION AND RECOMMENDATIONS 36
5.1 Introduction 36
5.2 Summary 36
5.3 Conclusion 38
5.4 Limitations of the Study 39
5.5 Recommendation for Further Research 40
REFERENCES 42
APPENDICES 47
Appendix I: List of Insurance Companies Underwriting Medical Insurance 47
Appendix II: Questionnaire-Insurance Industry 48
Appendix III: Introduction Letter to Respondents 49

LIST OF TABLES

Table 4.1 Descriptive Statistics..23

Table 4.2 Correlation Analysis……………………………………….23

Table 4.3 Model Summary...14

Table 4.4 ANOVA..24

Table 4.5 Coefficients..25

LIST OF ABBREVIATIONS

AKI:	-	Association of Kenya Insurers
AAR	-	African Air Rescue insurance company
AIG	-	American international group insurance
APA	-	Apollo and Pan African insurance company
BRITAM	-	British American Company
CIC	-	Co - operative Insurance Company
E & Y	-	Ernest and Young
IAIS	-	International Association of Insurance Supervisors
ICEA	-	Insurance Company of East Africa
IRA	-	Insurance Regulatory Authority
ISA:	-	International Standards of Auditing
KPMG:	-	Klynveld Peat Marwick Goerdeler
NHIF	-	National Hospital Insurance Fund
PWC:	-	Price Water House Coopers
KSH	-	Kenya Shillings
SMART	-	Simple, Measurable, Attainable, Reliable & Timely
UAP	-	Union and Provincial insurance

ABSTRACT

It is a common consensus that in the recent past there has been a tremendous growth in the number and value of cases reported involving fraud especially in insurance industry. Medical and Motor insurance business segments – the mainstay of the insurance industry, are said to be making loses as a result of increased fraud cases. AKI 2010 report found that the health insurance sector made the highest loss percentage of 81.5% followed by motor private insurance at 74.9%. This study had an objective of establishing the relationship between biometric technology and fraud in medical insurance firms. Data from year 2013 to 2015 was collected from 18 insurance companies that underwrite medical insurance business. The study adopted descriptive survey and data from insurance firms was collected by administering of a questionnaire. Data on value of fraud cases was collected from Insurance Fraud Investigation Unit. The study findings indicate that the value of reported fraud cases significantly increases with the value of claims authenticated via biometric technology. The main conclusion was that biometric technology has not had a negative impact in curbing fraud in medical insurance companies especially on claims submitted. The reason behind this is that as technology develops fraudster tactics become more advanced and complicated which has seen a rise in other forms of fraud like; cyber fraud, money laundering and internal fraud which cannot be prevented by use of biometric technology. However, it was found that biometric technology has really enhanced service delivery within the medical insurance sector especially by way of managing member benefits this can be shown from the model where there is a negative relationship between fraud cases and gross written premiums from members enrolled on biometric technology. The researcher therefore recommends that insurance companies to strengthen their internal control systems, improve corporate governance structures and ensure that they have internal and external audit functions as these are the key functions that can contain the fraud risk. The researcher also recommends a same type of study to be carried out in commercial banks.

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

Fraud is commonly known as lying, cheating and stealing. Ernst and Young (2009) define fraud as a deliberate action committed by a person or group of persons, who know that such actions can make them benefit unlawfully. Ramsay et al (2007) states that fraud is intentionally making material misrepresentation of fact, with the intention of inducing someone to believe and act on the falsehood, thus, incurring damage or suffer a loss.

The Association of Certified Fraud Examination (2014), categorizes fraud that affect organizations into three main classes namely; financial statement fraud, asset misappropriation and corruption. Fraud is therefore not confined to large companies nor is it confined to top executive; it can be done against customers, creditors, investors, in both private and public companies and even in the government. We can say that every business whether small or big is prone to fraud. With most companies trying to automate their processes, fraud can take place anywhere within the system either in the input or output level. It is that more often, fraud is discovered by reactive measures rather than proactive measures.

The most famous fraud as far as effect on business community is concerned, probably is the Enron scandal in 2001. Enron Corporation filed for bankruptcy after discovering significant misrepresentations in revenue and liabilities in its financial statements. By 2002, due to the outcome of the Enron scandal, Audit firm Arthur Andersen came to an end. In that same year, the U.S congress passed into law the Sarbanes-Oxley act (SOX) as a result of Enron's fraud case and others, such as WorldCom (Singleton & Singleton, 2010).

In 2013, Association of Kenya Insurers carried out Medical Insurance Fraud Survey. From the findings of the survey, different types of health insurance fraud were found to exist in the country but diagnosis manipulation; membership substitution, fee splitting, over servicing; provision of generic drugs instead of branded; pharmacy related; non-disclosure of prior ailments; and falsifying claims or altered invoices were found to be the most common forms of fraud in the sector. Health Service Providers were also identified as the major perpetrators of health insurance fraud.

1.1.1 Biometric Technology

Biometrics technology refers to authentication techniques that rely on the use of individual traits to access information data systems (Liu et al., 2001). Biometric technology is mostly used for identification and access control processes. Jain et al (2004) defines biometric as human body's unique (personal) physical or logical traits or characteristics.

Biometrics authentication occurs in two stages: on the first stage, the user's biometric trait is captured so it can be used in his or her authentication. After it has been captured, the user's trait is converted into a mathematical model, known as template, which is then submitted for authentication. On the second stage of biometrics authentication, the user's biometric trait is compared and validated as a stored template (Smart Cards and Biometrics in Healthcare Identity Applications, 2012).

There are four most common biometric techniques. The first one is Face recognition where the systems study the geometry and the proportions of the face (Vigliazzi, 2003). Second is Iris recognition which studies complexity of Iris tissue image and its radial pattern which are unique from individual to individual (Vigliazzi, 2003). Third is Voice recognition which is based on the fact that the physical traits of an individual entails to the singularity of the human voice as a feature (Magalhaes, 2003) and finally digital finger print technique which studies valleys and ridges on the finger's surface (Viola, 2006).

The choice of a biometric for any application depends on its characteristics like enrolment convenience, distinctiveness, universality, and also the application requirements like, accuracy, cost, speed, and robustness to fraudulent methods and attacks (Jain, Ross & Pankati, 2009).

The adoption of biometric technology is rapidly increasing around the globe due to the increasing sensitivity of security issues, and secondly it can easily be used with financial organizations like banks on use ATM Machines and approving of payment transactions, at retail locations on smart cards, credit cards, and anywhere you may make a financial transaction like in the health and social service programs, passport programs, driver licenses, and law enforcement (Siddiqui & Muntjir, 2013).

1.1.2 Fraud in Insurance Industry

Insurance Fraud isn't a new thing; it has always been in existence wherever underwriting of insurance policies is done, and it has taken different forms and dimensions to fit the economic time and coverage available. Derrig and Kraus (1994) define insurance fraud as unlawful acts which are provable beyond reasonable doubt and that violate laws by making the intentional acts of obtaining money or gain from the insurer under false pretense or material misrepresentations. It is characterized as being diverse in its make-up, easy to commit and with a low risk of detection (Goetz, 2011). Clarke (1990) notes that insurance firms' own reluctance to respond effectively to the problem of fraud has led to increase in fraud in the insurance sector.

Risk in the insurance value chain can stem from internal or/and external factors. Internal fraud is on the rise where employees are misusing confidential information and colluding with fraudsters requiring insurers to lay down strong internal control systems to mitigate such issues. External fraud risk in insurance companies can emerge at various stages such as when capturing of clients details in systems, during underwriting of the insurance business, reinsurance and the processing of claims.

Gill (2001) notes that, the body of knowledge around insurance fraudsters is shallow and is complicated by the finding that most of those who commit insurance fraud have no knowledge or agree that they are committing an offence. In the study of insurance fraudster profile, Button et al (2013) found that the household insurance fraudster to be almost as likely male as female (54:46) aged 30-50 years with a mean age of 44, and from a variety of occupations.

Levi (2008) has noted of fraud generally, but it is equally applicable to insurance fraud, that some types require specialist skills (and to this may be added access to networks of suitably qualified co–offenders), while other types of fraud, involving low levels of skill, may be committed by ordinary people, for example by adding items to others legitimately taken in a burglary.

There are three principal categories of insurance fraud according to Association of British Insurers (2012). First is opportunistic fraud in retail and general insurance which include inflated and counterfeit claims. Second is opportunistic fraud in commercial insurance where focus is on organizations committing fraud rather than individuals. Third is organized fraud involving gangs. Clearly, there is a substantive difference between opportunistic fraud, where people encounter an opportunity within their everyday experiences to commit fraud and more organized planned frauds. Insurers may also be victimized by their own staff that are looking up opportunities to commit fraud and/or are planning to commit the heinous act, and sometimes work with outsiders.

1.1.3 Biometric Technology and Fraud in Medical Insurance Firms

Insurance fraud is a major issue across the whole insurance value chain, most affected areas being underwriting and claims. As technology advances, fraudster tactics become increasingly advanced and complex, insurers have to deal with other new forms of fraud like, internal fraud, cyber fraud and money laundering.

The Fraud Triangle theory explains that fraud is made up of three main elements; perceived pressure, perceived opportunity and rationalization of the act of fraud (Albrecht et al. 2009). Medical insurance firm's employees have knowledge of the systems as well as classified and confidential information which together with technological advancement can give them the opportunity to commit frauds. All they need is some pressure and the rationalization and that way they become part of fraud cartels that are fleecing millions of shillings from the insurance companies.

As stated in the Insurance Regulatory Authority's fourth quarter report 2015, 106 suspicious cases were reported to the Insurance Fraud Investigation Unit (IFIU) in year 2015, up from 87 cases in 2014. The amount lost due to fraud increased by 257% i.e. from Kshs 102.76 million in 2014 to Kshs 366.90 million in 2015. Of the 106 cases reported, motor vehicle underwriting was at the top of the list with 42 cases followed by broker/agent fraud at 25 and then medical fraud with 17 cases. But the problem with fraud data is that cases often go unreported. Rittenberg et al (2008) estimates that 40% of the fraud cases have been uncovered but not prosecuted and an additional 40% of fraud cases have not been discovered.

Use of biometrics for identification can be defined as assessing of an individual's identity using unique physical or behavioral trait (something that is uniquely theirs). For years, people have been identified based on something they own or given to them to identify those examples being identity cards, birth certificates, tokens or something they master like personal identification numbers (PIN) or passwords. Digitized biometrics have many advantages as compared to physical tokens and numerical codes; they are unique to each individual, cannot be lost or forgotten, cannot be stolen and are impossible to forge, do not require any form of literacy, can help create an auditable trail for transactions and finally, can increase anonymity when used in place of personal details e.g. names, addresses, etc. (Jain et al, 2004).

Tistarelli and Nixon (2009) points out that the use biometric technology is an effective means in curbing fraud since it uses unique characteristics, easy to install and requires little amount to purchase the equipment. Biometric technology also has an advantage of being less prone for users to share access of highly sensitive data making it a secure way of identifying users. Each person's unique identification is used as the single most operative identification for that user. Chances of two users sharing the same identification in the biometrics security technology are almost zero.

1.1.4 Medical Insurance Firms in Kenya

Medical Insurance firms in Kenya, like other insurance companies, are regulated by Insurance Regulatory Authority (IRA) and operate under an umbrella body called Association of Kenya Insurers. As at December 2014, Kenya had 29 licensed medical insurance providers and the top 10 are; Jubilee Insurance, AAR Insurance, APA Insurance, UAP Insurance, GA Insurance, Britam Insurance, Saham Insurance, Madison Insurance, CIC Insurance and Resolution insurance. In year 2011, IRA established Insurance Fraud Investigative Unit to handle cases of fraud in the insurance industry, and the unit collected reports and investigated cases of insurance fraud totaling to 87 during the year 2014 as compared to 57 similar cases in 2013.

At the top of medical insurance firms are three re-insurance companies. Among the three, Kenya Reinsurance Corporation is a publicly traded company while East Africa Reinsurance Company Limited and Continental Reinsurance Company Limited are privately owned companies. The three re-insurance companies also offer re-insurance services to other insurance companies in the industry.

Medical insurance business, the fastest growing insurance category in terms of premiums ranks second after Motor insurance with 15% of industry's Gross Written Premium (GWP). In year 2014, according to AKI 2014 report, the industry reported GWP of Ksh 25.31billion a growth of 20.95% compared to year 2013, and in year 2013 it recorded a growth of 60.09% compared to year 2012. Despite the recording a growth in premiums, the medical class has challenges with profitability where almost three quarters of the medical insurance firms are doing loses. Some of the major challenges facing the industry are the poor pricing of medical products, low uptake of medical cover as medical cover is not of priority to majority of Kenyans, fraud and high costs of healthcare. In an attempt to mitigate the segment's risk exposure, companies have introduced co-pay systems in which the underwriters share costs, such as hospital administration, with policyholders. New technology, including biometric identification systems, is also expected to reduce the incidence of medical insurance fraud.

1.2 Research Problem

According to the survey carried out by Ernst & Young (2011), fraud risk presents a very huge challenge for the insurance sector affecting parties involved i.e. insurers and policyholders. Fraud has led to increase in the cost of insurance, leading to insurers losing to their competitors, and at the same time policyholders paying higher premiums. It is estimated that between 20% and 40% of the claims in medical insurance are usually fraudulent, forcing the insurance companies involved in medical insurance underwriting to incur massive loses. So grave is the situation that three quarters of the medical insurance firms are making loses.

Angima and Omondi (2016) notes that; frauds in the health care system include, pocketing of user fees by service providers or overcharging of health insurance benefits by doctors. Within the hospital, it could involve the diversion of patient fees or collusion between hospital administrators and sending of fake claims to insurance companies.

In view of these fraudulent activities in the health insurance in Kenya, Health Data Systems Limited launched the use of smart medical cards which uses fingerprint biometric technology. The aim was to eliminate fraud in healthcare at the point of service. Patients will not be able to falsify or forge their identities, and it helps deter dishonest providers from submitting bogus claims. Use of biometrics to identify patients creates an audit trail that is irrefutable which can prove and confirm the patient's identity at the time of service eliminating fraudulent billing hence bringing a greater degree of accountability and transparency in the health care billing process. Biometrics support preemptive approach that offers a more proactive strategy for thwarting healthcare fraud before claims are paid. The technology has also an advantage of monitoring the individual members benefits since it is a real time process hence issue of where the member exceeds benefits is completely eliminated.

Mulumba (2012) studied biometric authentication systems and service delivery within the healthcare sector while Wanjiru (2012) studied the strategic responses to increasing fraud related risks. Ngakyuka (2013) conducted a research to determine the relationship between ICT and fraud in commercial banks in Kenya. Onywoki (2014) too looked into the framework for the adoption of biometric ATM authentication in Kenyan financial institutions. No study has been done on the effectiveness of use of biometric technology utilization to curb fraud in medical insurance companies.

UAP insurance was the first medical insurance to use Biometric technology but as at now more than 70% of the medical insurance companies have adopted the technology. Given the enormous use of the biometric technology in medical insurance firms in Kenya and across the world, the study aimed at determining the effectiveness of use of biometric to curb fraud in medical insurance firms. This study sought to answer the question; is the use of biometric technology effective in curbing fraud in medical insurance firms in Kenya?

1.3 Objective of the Study

The objective of this research is to ascertain the relationship between biometric technology and fraud in medical insurance firms in Kenya.

1.4 Value of the Study

This study looks into the effectiveness of use of biometric technology to curb fraud in insurance industry. Fraud leads to a general increase in the cost of healthcare due to rising insurance costs, resulting in inability to afford medical covers. Fraud also affects the rate of penetration of medical insurance because the cost is not affordable. This study is going to confirm if indeed application of biometric technology is effective in curbing fraud in medical insurance firms.

The government can use the findings to formulate laws on fraud and also design procedures relating to use of biometric technology especially in areas where authentication is required. Scholars and other researchers are also likely to benefit from this study as they will use the findings for future references and will also be able to compare facts.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter gives a literature review on topics same and similar to this topic together with other similar topics. The available literature will help in improving on the methodology used and also be used in providing a critical analysis.

2.2 Theoretical Framework

Four theories are relevant in explaining fraud in medical insurance firms. They include the Fraud Triangle theory, The Fraud Diamond Theory, Fraud scale theory and The Economic Contractual Theory. These theories will be discussed as below;

2.2.1 Fraud Triangle Theory

This theory was advanced by Donald Cressey in 1950. The Fraud Triangle theory uses three main elements to explain what motivates fraud namely; perceived pressure, opportunity and rationalization.

The first element necessary for fraud to occur is pressure. Pressure is taken as a critical factor to commit fraud and the three main types of pressures are employment stress pressure, personal pressure and external pressure (Lister, 2007). According to Vona (2008), the main motivating agents that lead to commitment of fraud are corporate and personal pressures. Some examples of perceived pressure include being greedy, living beyond one’s means, having large expenses or personal debts, addiction to drugs, family health problems and financial difficulties. Albrecht et al (2006) notes that it’s important to use the word perceived as pressure is sometimes not be real; if the perpetrator thinks and believes that they are under pressure, this thinking can make them commit fraud. The perceived pressure can come out from different kinds of settings, but in most cases it will involve non-sharable financial need. The most common type of pressure which impact on most employees is the financial pressure and it has a serious impact on employee's motivation. Specifically, according to Albrecht et al (2006) financial pressure has been the reason behind around 95% of fraud cases.

Perceived opportunity is the second element of the Fraud Triangle Theory. Rae and Subramanian (2008) refers to opportunity as a weakness in the business system where an employee has the power or chance to maximize on the weak line and hence commit fraud (Rasha & Andrew 2012). It always works that if the risk of being napped is low, then the high chances are that fraud will take place (Cressey, 1953). According to Sauser (2007), there exist other factors that contribute to fraud and they relate to perceived opportunity and they include: a believe that the employer is not informed or aware, a believe that employees are not regularly checked on violating the organization policies and regulations, the assumption that no one cares, and that nobody will take into consideration that the act of committing fraud to be a serious offense.

The third element is for fraud to occur is rationalization. Rationalization refers to where an individual tries to justify that his or her unethical behavior is not a criminal activity. Hooper and Pernelli (2010), notes that people who commit fraud, always have a mind-set that allows them to excuse or justify their fraudulent activities.

2.2.2 The Fraud Diamond Theory

This theory is similar to Fraud triangle theory except an element capability has been included and was presented by Wolfe and Hermanson in the CPA Journal (December 2014). The argument of Wolfe and Hermanson (2004) is that, even if the perceived pressure or incentive is likely to co-exist with a chance to doing fraud and a justification for committing the fraud, it's not likely that fraud will be committed without an existence of the fourth element i.e. capability. In other way, a person committing fraud must have all knowledge and skills that can enable him or her to commit fraud.

The elements of Fraud Diamond Triangle are interrelated to the extent that an employee cannot commit fraud until all of the elements are present. The theory proposes that pressure can lead someone to look for an opportunity, and pressure and opportunity can encourage rationalization. At the same time, none of these two factors, alone or together, necessarily cause a person to engage in activities that could lead to fraud until the fraudster has the capability to do so (Hooper & Pornelli, 2010).

2.2.3 The Fraud Scale Theory

The fraud scale theory was advanced by Albrecht, Howe and Romney (1984) as an alternative to fraud triangle model. The two theories i.e. the Fraud scale Theory and Fraud Triangle theory are very similar; however, the only thing that separates the two theories is the use of an element of Personal Integrity instead of rationalization. Personal integrity element is usually associated with a person's personal code of ethical behavior. It is observable in both a person's decisions and the decision-making process unlike rationalization in the fraud triangle, which according to Albercht et al, (1984) can assist in assessing integrity and finding out if a person is likely to commit fraud.

The argument is in line with other researches. Professionals concur that fraud and other behaviors which are not ethical often are as a result of an individual lack of integrity or other moral reasoning (Dorminey et al., 2010 & Subramanian, 2008), as moral and ethical norms are vital roles in person's decisions and judgment.

2.2.4 The Economic Contractual Theory

This theory was advanced by Hart and Moore (1988). It suggest that insurance fraud happens within the context of a contractual relationship between the insurer and the insured, hence viewed as purely economic response to this contract. The way fraud is viewed here builds on economic theories of moral hazard, which seeks to recognize that insurance reduces the insured's incentives not to incurred losses, and exaggerated or bogus claims are characterized an ex-post moral hazard.

The traditional economic theories of crime dictate that; when a person is making a decision to lodge a fraudulent claim they will have weighed between the magnitudes of successfully gaining from the filing against the severity of the consequences from the act. If a person finds that the gain from fraud is more than the consequences a person will suffer then, the individual will lodge a fraudulent claim (Mazar, et al. 2007)

2.3 Determinants of Fraud in Medical Insurance Firms

There are several factors that determine fraud in medical insurance companies. These are discussed below under three main categories; Weak Internal control system, Lack of internal and external audit functions, and poor corporate governance structures.

2.3.1 Weak Internal Control Systems

Failures to avert and unearth fraud have serious repercussions to companies. Fraud can be minimized by putting in place control systems that can help management. Internal control system is highly regarded as a key deterrent in committing of fraud (Omar et al., 2015). Internal control systems can be defined as the whole system of control; financial or otherwise that the management designs and maintains so as business is carried out in orderly and efficient manner with an overall objective of achieving the companies' objectives.

Internal Controls according to Benjamin (2001) include all the policy and procedures maintained by the directors and management of a company to enable them meet their set objectives, which includes adhering to internal policies, safeguarding of the company's assets, preventing and detecting of fraud and error as well as the completeness and accuracy of records, with preparation of reliable and accurate financial information in a timely manner.

2.3.2 Lack of Internal and External Audit Functions

Audit is the examination and reviewing of the companies' systems, processes, projects or products, which usually involves an independent and a fair assessment of the financial statements of an entity. Cameron (1982) defines external auditors as experts who carry out audit examination of on the financial statements or books of account of an individual company, legal entity or even the government itself. The main difference between internal audit and external audit is; internal audit will usually evaluate issues that relate to the organization's business practices and risks, while external auditors tend to review the financial records and give an opinion the financial records of the organization. External audit are usually conducted at year end while internal audits are usually a continuous process conducted throughout the year.

Both internal and external audits work independently to give a fair opinion on the financial statements and processes of a company. Monaghan (1989) states that an Independent auditors' duty is to discover misstatement and any errors which are material, this include fraud, the independent auditor occupy a role that the public considers it to be most significant especially in the evaluation of the company financial statements. Lack of Internal and external audit functions in any medical insurance firms will definitely point out to high chances of fraud occurrence.

2.3.3 Poor Corporate Governance Structures

Corporate governance as defined by Sifuna (2012), is system of law and sound approaches by which companies or business entities are governed and managed with a focus on the internal and external corporate structures with the intention to monitor actions of the management and directors as well and hence limiting agency risk which can result from the misdoings of the company or organization officials.

Corporate governance is a structure that is all about who controls companies and why. In addition, good governance is also required to ensure ethical conduct and socially responsible behavior (Allaire & Firsirotu, 2003). Besley (1996) found that when a larger number of the board are outsiders, financial reporting is greatly reduced but he didn't find much evidence that there was less frequency in meetings by audit committees of the affected companies. According to Ramaswamy (2005), poor corporate governance and failure in accounting is one of the major reasons why fraud cases come up. The reason being that poor corporate governance gives room for individuals or group of people to with the same interest to do fraud or carry out fraudulent activities within a corporate. He also mentions that another reason why fraud cases emerge is problems within corporate reporting system. This implies that to govern a corporate more effectively must be an outcome of transparency and best practices on one hand and consistent healthy profits for all other individuals involved on the other (Agarwal & Medury, 2013).

2.4 Empirical Studies

Prior studies of insurance fraud have concluded that medical insurance fraud is easy to commit and is justified by those who do and often go undetected. Angima and Omondi (2016) examined the nature of fraud and its effects in the medical insurance sector in Kenya. The study aimed at determining the nature of fraud patterns and its effect in the medical insurance industry in Kenya and to establish possible solutions in countering fraud in the medical insurance subsector in Kenya. Descriptive cross sectional research design was adopted and the finding showed that to curb fraud; customers to produce medical cards when they visit hospitals, subject claims to audit to determine validity, adoption of modern technologies in the management of database within the organization.

Abiola (2013) did an analysis on the Impact of information Communication Technology (ICT) on internal control's prevention and detection of fraud. Using a triangulation of questionnaire and interview techniques to investigate the internal control activities of Nigerian Internal Auditors in relation to their use of ICT in fraud prevention and detection, the study made use of cross-tabulations, correlation coefficients and one-way ANOVAs for the analysis of quantitative data, while thematic analysis was adopted for the qualitative aspects. The study's findings show that Nigerian Internal Auditors are increasingly adopting IT-based tools and techniques in their internal control activities. The study also found the use of ICT – Based tools and techniques in the internal controls positively impacts on Internal Auditors' independence and objectivity. Also the results indicate that internal auditor's use of ICT – Based tools and techniques has the potential of preventing electronic fraud, and such ICT-based tools and techniques are effective in detecting electronic fraud

Mulumba (2012) studied the biometric authentication systems and the service delivery in the healthcare sector in Kenya. The objective of the study was to determine the factors that affect performance of biometric in the healthcare system and its impact in delivering services. The study, that employed descriptive survey approach, was carried within Nairobi and it involved 43 healthcare facilities that were using biometric systems. Using conceptual model, the study found that ease of tracking medical benefits usage and reduction of financial loss through fraudulent claims were the main positive impact of the systems. From the research, it was concluded that biometric is used for identification purposes and also for billing services and it doesn't alter the quality of the service delivery.

Makori, Nyagol and AJowi (2016) undertook to study the influence of internal control system on fraud risk management among commercial banks in Kisii town, Kenya. The study had a purpose of examining the relationship between risk assessment and fraud risk management among banks in Kisii town. The study concluded that internal control systems have the greatest influence on the management of fraud risk among banks in Kisii town.

Kiragu, Gikiri and Iminza (2015) carried out a research to determine the effect of the bank size and the occupational fraud risk: With Empirical evidence from commercial banks in Kenya. The study sought to analyze impact of commercial bank size on occupational fraud risk in Kenya and provide appropriate understanding into the importance of organizational size in occupational risk deterrence. The study found a negative relationship existed between organization size and risk of fraud meaning the larger commercial banks have ability and are always implementing greater controls as compared to smaller banking hence chances for larger banks being affected by fraud are greatly minimized.

Coalition against Insurance Fraud (2014) carried out a study of insurer use, of strategies, and plans for antifraud technology. The objective of the study was to better understand how insurers are using technology to tackle and curb insurance fraud. The study concluded that anti-fraud strategies will include the right choice of tools and technologies will lead to high fraud detection rate and prevention thereafter. The strategy will in turn significantly help in lowering down overall losses for the insurer and which is more likely to translate to accurate pricing, competitive edge and lower premiums for policy holders. This will in turn lead to increase in insurance penetration.

Ngalyuka (2013) carried out a research on the relationship between Information communication technology Utilization and fraud loses in commercial banks in Kenya. Secondary data was used for this research and was collected from Central Bank of Kenya reports and Bank Fraud Investigation Unit reports and audited financial statements for all the 43 registered commercial banks in Kenya. It was found out that level staff costs contributes a lot on the fraud losses at the commercial banks followed by ATM transactions and EFT transactions respectively.

Kisaka (2012) sought to find out fraud investigation and detective framework in the motor insurance industry; a Kenyan perspective. The research design involved the linking of research questions to empirical data. The target population consisted of 46 insurance companies. It was found that the predominant form of insurance claims across the global industry revolves around health insurance. Motor claims fraud came second with property insurance claims fraud third

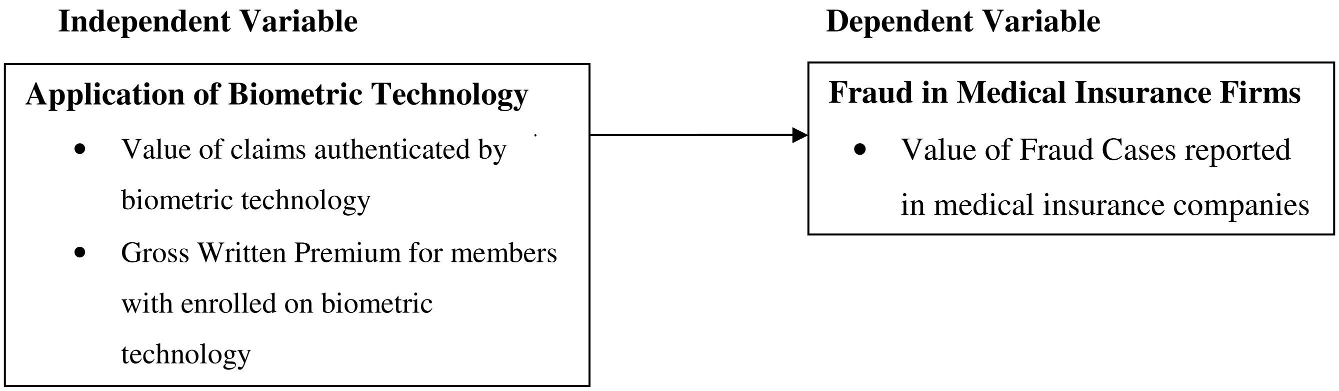
Akelola (2012) researched on Fraud in the banking industry; A case of Kenya. The research mixed both qualitative and quantitative study and was based on thirty banks across the industry. The study also focused on fraud and security managers who gave responded to questionnaires. The research had a conclusion that fraud is still considered to be a major issue in banking industry, although their relative size of fraud committed was relatively small and unsophisticated.

Sitienei (2012) examined factors that influence credit card fraud in the banking sector, case of commercial banks in Mombasa. The study looked to find out the factors influencing credit card fraud in the banking sector. The study found that credit card skimming, technology; system security, proper card management and system integration as the main factors that were given high priority in influencing credit card fraud in the banking sector. The study further recommends adoption of smart credit cards by all banks as their main mode of operation; smart card usually operate the same way as their magnetic counterparts and the only difference being that an electronic chip is usually embedded in the card which can be loaded with the customer's biometric details.

2.5 Conceptual Model

Conceptual model defines the connection between the dependent and independent variable. The dependent variable is value of cases in medical insurance firms while the independent variables are value of claims authenticated by use of biometric technology for past three years and gross written premiums from members enrolled on use of biometric technology.

Figure 1: Conceptual Model


Independent Variable
Dependent Variable
Application of Biometric Technology
• Value of claims authenticated by biometric technology
• Gross Written Premium for members with enrolled on biometric technology
Fraud in Medical Insurance Firms
• Value of Fraud Cases reported in medical insurance companies

2.6 Summary on Literature Review

The chapter had an aim of giving a literature review related to the motive of the study. The main purpose of this study was to find the effectiveness of use of biometric technology in curbing fraud in insurance firms in Kenya. It's evident from the different works of the authors mentioned above that the severity and extent of insurance fraud tends to range from a simple submission of a fake claim to intentionally making of huge losses of insured assets. The main basic elements of fraud are the intention to deceive and the willingness to make a company pay than it ought to have paid. It's therefore paramount that the medical insurance companies, government and other organization should engage in the use of biometric to weed out fraud. Insurers also need to employ qualified fraud and investigation staff that can work together with law enforcement agencies to pick out fraudulent activities. The industry should also build a centralized database to share the information that relates to fraud.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

We noted in chapter one that this research seeks to determine the effectiveness of use of biometric technology to curb fraud in medical insurance firms in Kenya. In this chapter we will discuss research procedures and the methods that were employed in conducting the study. Research methods will be discussed as well as design that was employed. Also the population, sampling technique and methods that were employed in collecting data and finally the data analysis approach taken will be discussed.

3.2 Research Design

Research design is defined to be a complete set of decisions that creates the main plan which specifies the procedures together with the methods methods that will be used to collect and analyzing the information needed. Kothari (2004) states that a research design directs the researcher by offering guidelines on how to data should be collected, analyzed and thereafter interpreted in a coherent manner

A descriptive survey was applicable in this study as such a design, according to Cooper and Schindler (2003), seeks to answer the questions, where, how much, what and by what means the research will be conducting, Another reason for use of descriptive survey was that a broad range of information in regarding utilization of Biometric technology and fraud in medical insurance firms in Kenya was required in the study

3.3 Population

According to Hair (2003), population is defined as totality of elements or an identifiable total group which are of interest to a researcher and applicable to the specified information problem. In this case the target population is composed of 18 medical insurance companies (see Appendix 2). The target population was sourced from the Insurance Regulatory Authority and Association of Kenya Insurers.

3.4 Data Collection

Kothari (2004) describes collecting data as a process of putting together the empirical evidence so as to understand the new information a condition or a situation and be able to answer questions that are necessitated by the research to be undertaken. The researcher used both primary and secondary. In collection of primary data, a questionnaire was used while secondary data was collected from Insurance Regulatory website (IRA). Data on Fraud was collected from Insurance Fraud Investigation Unit (IFIU) and the insurance companies as well.

3.7 Data Validity and Reliability

Validity is basically involved to which extent or how far an instrument is measuring what it is supposed to measure. To test for data validity as well as data reliability, a pilot survey was done. Researchers from different institutions that do research and also various universities were given draft questionnaires for their independent review on the factorial criterion.

3.5 Data Analysis

To allow for statistical analysis, a completed questionnaire was edited for consistency and completeness and also coded was done. According to Mugenda (1999) data should be clearly coded and well analyzed so as to get a relevant report.

The data collected was analyzed and interpretation done use Statistical Package for Social Science (SPSS version 22). And to quantify the relationship between the dependent and independent variable, the regression analysis was used. Results were then presented in form of tables to aid in the analysis.

3.5.1 Analytical Model

Multiple linear regression equation that was used took into consideration two independent variables for the 18 insurance companies from year 2013. It was presented as follows;

$$\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \varepsilon} \text{ .... } \mathbf{(2)}$$

In order to measure the dependent variable (Y) the researcher used the value fraud cases in the medical insurance firms. The researcher looked to establish the relationship between the value of fraud cases reported (dependent variable) and the level of usage of biometric technology (smart Cards) i.e. claims authenticated by use of smart and Gross written premiums from members with smart cards.

Where;

Y = the value of fraud cases in medical insurance firms for past 3 years

β_1, β_2 = Coefficients of determinations / the slope of the curve

$\boldsymbol{\beta_0}$ = constant/Y intercept

$\mathbf{X_1}$ = Gross Written Premium from members enrolled on biometric technology for the 18 insurance companies for past 3 years

$\mathbf{X_2}$ = Value of claims authenticated by use of biometric technology (smart cards) for 18 companies for the past 3 years

$\boldsymbol{\alpha}$ = the values of an unobserved error term.

3.5.2 Test for Significance

The coefficient of determination (R^2) was used in measuring the extent or level to which the variation in value of fraud cases is explained by the variations in use of biometric technology. F-statistic was also be computed at 95% confidence level to test whether there is any significant relationship between use of biometric technology and the value of fraud cases reported

CHAPTER FOUR

DATA ANALYSIS RESULTS AND DISCUSSION

4.1 Introduction

The chapter represents data analysis, results and discussion of the research finding as laid down in the research methodology chapter. The research was done on two main elements indicating the usage of biometric technology namely; Gross written premiums from Members enrolled on smart technology and value of claims authorized by use of biometric technology from year 2013 to 2015.

4.2 Descriptive Statistics

Descriptive statistics are shown in the below table 4.1 and they include the mean and standard deviation. The statistics were computed for 18 insurance companies annually between 2013 and 2015.

Table 4.1 Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Variance	Skewness	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error
Gross Written Premiums from members on biometric Kes. '000000	54	0	13387.3	1001	2007.312	4029302	4.775	0.325
Claims authenticated via Biometric Technology Kes. '000000	54	0	12616	895.1	3360.595	11293598	6.89	0.325
Value of fraud cases reported Kes.'000	54	0	7861	652.3	1729.765	2992087	3.068	0.325
Valid N (list wise)	54							

Fig 4.2 analysis the descriptive statistics for the three quantitative variables, value of fraud reported, gross written premiums and claims authenticated through the biometric technology in the 18 major insurance companies in Kenya offering medical policy.

4.3 Correlation Analysis

The table below shows correlations between the three variables that is value of fraud cases reported, gross written premiums and the claims authenticated through the Biometric Technology (BMT)

Table 4.2 Correlation

		value of fraud cases reported	Gross written premiums	Claims authenticated via smart
value of fraud cases reported	Pearson Correlation	1	0.093	.409**
	Sig. (2-tailed)		0.506	0.002
	N	54	54	54
Gross Written Premiums From Members on Biometric Technology	Pearson Correlation		1	0.25
	Sig. (2-tailed)			0.068
	N		54	54
Claims authenticated via Biomtric Technology	Pearson Correlation			1
	Sig. (2-tailed)			
	N			54

Source: Research Findings

The total number of cases (N) was 54, the dependent variable is the value of fraud cases reported between 2013 and 2015 and the independent variables are the GWP and the claims incurred in the same period.

This shows Pearson correlations, r, in the first row and significance of the correlation in the second row. R values along the diagonal line in the table are 1 because it is the interaction of the variable with itself.

4.4 Regression Analysis

The below model was developed after doing analysis of the data

Table 4.3 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.382[a]	.146	.112	1700.23025

When the predictors are kept constant, that is claims authenticated through biometric technology and the gross written premiums and the outcome variable being value of fraud cases reported there was a moderate correlation amongst the variables, (R 0.382).

Table 4.4 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	26584211.321	2	13292105.661	5.136	.009[b]
	Residual	131996411.938	51	2588164.940		
	Total	158580623.259	53			

a. Dependent Variable: value of fraud cases reported

Table 4.4 Analysis of Variance

Table 4.4 analysis of variance indicates F-STATISTIC at 5.136 with an average mean square at 13292105.7 at significant p=0.009, which means that the variation in the dependent variable is explained by the model is not just by chance or in other words the results show statistically significant differences and linear relationships amongst the gross written premiums and claims authenticated via the biometric technology system

Table 4.5 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	471.643	247.199		1.908	0.062	-24.629	967.916		
	Claims authenticated via Biometric Technology	0.212	0.068	0.412	3.122	0.003	0.076	0.348	0.937	1.067
	Gross Written Premiums from Members on Biometric Technology	-0.009	0.114	-0.011	-0.08	0.936	-0.237	0.219	0.937	1.067

a. Dependent Variable: value of fraud cases reported

Table 4.5 Coefficients Correlation, the results show statistically significant differences and linear relationships amongst the gross written premiums and claims authenticated via the smart system. This is a clear indication that the impact claims have on the value of the fraud cases reported is unrelated to that of gross written premiums. Therefore this shows that the relationship between variables is significant at F (2,51)=5.236.

$\mathbf{Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \varepsilon}$ **..................** becomes

Y= 472- 0. 009 $\mathbf{X_1}$ +0.212 $\mathbf{X_2}$

where

Y, dependent variable= value of fraud cases reported

B_o coefficient constant in the table above

B1 coefficient for X1=value of gross written premium

B2 coefficient for X2 =value of claims authenticated through smart.

The regression equation therefore:

The data shows that the value of the dependent variable Y, value of fraud cases reported, will vary with the independent variables X1 and X2 as per the equation above.

Table 4.6 Collinearity Diagnostics[a]

				Variance Proportions		
Model	Dimension	Eigenvalue	Condition Index	(Constant)	claims authenticated via smart	gross written premiums
1	1	1.701	1.000	.16	.14	.17
	2	.759	1.497	.26	.81	.04
	3	.541	1.774	.58	.06	.79

a. Dependent Variable: value of fraud cases reported

Source: Research Findings

Table 4.6 Co-llinearity diagnostic shows variance proportion of .14 and .17 for the independent variables claims and gross written premiums respectively. The Eigenvalues are far from 0 which shows that there is low level of multi-collinearity between the predictor values

4.5 Discussion of Research Findings

Table 4.1 analyses the descriptive statistics for the three quantitative variables, value of fraud reported, gross written premiums and claims authenticated through the biometric technology in the 18 major insurance companies in Kenya offering medical policy. Data was collected annually for each of the insurer in terms of gross written premiums, claims authenticated through the biometric technology and the value of fraud cases reported for 2013, 2014 and 2015. This contributed to generation of 54 responses that were coded, processed and entered into SPSS for analysis.

The Gross written premium had a mean of Kes.1000 Million with a standard deviation (STD) of 2007 which can be due to variation in the value of gross premiums amongst different insurance companies. The test for data distribution shows an error of 1 below since the data was well distributed with a standard error of .325. The value of fraud cases had a mean of Kes.653 thousand with a slight standard deviation (STD) of 1730 and claims authenticated via the biometric system was having a mean value of Kes.895 Million and a standard deviation of 6.890. Data distribution is significantly appropriate within the table for use in statistical analysis. The results show that fraud cases have been in the rise in the health insurance sector. The same findings were also similar to that of Kisaka (2012) who sought to find out fraud investigation and detection framework in insurance firms in Kenya.

Examining the results above, the value of claims authenticated via the biometric system is related to the value of fraud reported via the same system, α=0.212, p=0.03. This value is positive and therefore indicates a positive linear relationship between the value of fraud reported and the amount of claims reported, if you increase claims there will be significant increase in the value of fraud reported. Fraudsters are always running a head of technology and innovating new ways to recover more claims and also get reimbursements even in the instances of voidable claims. This study has a same findings with that of Ngalyuka (2013) who was studying the relationship between usage of ICT and fraud in commercial banks in Kenya and she found that there exists a positive relationship between the usage of ICT and fraud losses reported by commercial banks.

The result also can be supported by the diamond theory argues that in addition to the perceived pressure, opportunity and rationalization to commit fraud the capacity to do so will also determine the likelihood of fraud occurring. The possibility of manipulation of system and procedures in order to commit fraud cannot be dispelled in the event that the experts in the business processes have financial pressure and there is an opportunity to commit fraud. Furthermore, proponents of literature on fraud have supported that some form of fraud requires specialists especially in the modern day technology.

The results also indicate that there was a negative relationship between the fraud cases reported and the gross written premiums from members enrolled on biometric technology i.e. the coefficient of the premiums is negative (-0.009) which means a relationship between the value of fraud and premiums will have a negative linear relationship. This can be interpreted as biometric technology has been effective in managing benefits for members. The findings were the same with Mulumbas (2012) who found that biometric technology has been effective in enhancing service delivery. Also by controlling billing process, biometric technology has been effective to some extent to curb fraud in that area.

Table 4.6 Collinearity diagnostic shows variance proportion of .14 and .17 for the independent variables claims and gross written premiums respectively. The Eigenvalues are far from 0 which shows that there is low level of multicollinearity between the predictor values. This further supports the results of the correlation which indicates non relationship between the gross premiums and value of fraud reported and moderate relationship between claims authenticated via biometric system and the value of fraud. In addition, the two predictor variables are not significantly related according to results in table 4.3. A change in one of the independent variables will have a slight change in the other.

In conclusion, the fraud scale theory adds personal integrity as one of the factors that motivates or discourages people from committing fraud. Fraudsters will always find loopholes to cheat or lie for unfair gains. The claims assessors in the medical underwriting are concentrating on the cover limits and validity of the clients in the system and forgotten that lack of integrity is causing the providers to collude with client and ends up billing wrong diagnoses, drugs and even overpriced services. There was more scrutiny of claims to determine viability before introduction of the Biometric system in the insurance industry. Insurers should understand that in as much as the system might have reduced cost of operations and improved business processes the fraudsters have also found easier ways of making money from the same.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter gives the summary of the findings from chapter four, conclusions, and limitations of the study and the recommendations which are based on the objective of the research i.e. to establish the relationship between biometric technology and fraud cases in medical insurance firms in Kenya

5.2 Summary

The study had an objective of determining the relationship between usage of biometric technology and fraud cases in medical insurance company. The study used descriptive survey and data collected annually between 2013 to 2015 from eighteen major insurances in medical underwriting. Data was coded, entered into the SPSS version 23, scanned for any errors and distribution and important analysis drawn from the data to support the study objective in relation to the theoretical framework.

There is a moderate degree of relationship between the claims submitted and the value of fraud reported. This supports the theory of Fraud Triangle theory which argues that fraud is as a result of interplay amongst three key principles perceived pressure, perceived opportunity and rationalization.

Looking at the coefficients results in fig 4.4.3 the gross written premiums is not significant, p=0.36, but the coefficient is negative -0.009 which would indicate that larger amount of premium is related to lower value of fraud cases reported. This could support the form of fraud cases that are regularly reported by the insurance companies. There are quite a number of fraud cases which attempts to interfere with the underwriting guidelines when it comes to calculation of premiums. The insured colludes with the underwriter and ends up paying lower premiums than expected. The diamond theory argues that in addition to the perceived pressure, opportunity and rationalization to commit fraud the capacity to do so will also determine the likelihood of fraud occurring. The possibility of manipulation of system and procedures in order to commit fraud cannot be dispelled in the event that the experts in the business processes have financial pressure and there is an opportunity to commit fraud. Furthermore, proponents of literature on fraud have supported that some form of fraud requires specialists especially in the modern day technology.

The value of claims authenticate via the biometric system is related to the value of fraud reported via the same system, $\alpha=0.212$, $p=0.03$. This value is positive and therefore indicates a positive linear relationship between the value of fraud reported and the amount of claims reported, if you increase claims there will be significant increase in the value of fraud reported. Fraudsters are always running a head of technology and innovating new ways to recover more claims and also get reimbursements even in the instances of voidable claims.

The fraud scale adds personal integrity as one of the factors that motivates discourages people from committing fraud. Fraudsters will always find loopholes to cheat or lie for unfair gains. The claims assessors in the medical underwriting are concentrating on the cover limits and validity of the clients in the system and forgotten that lack of integrity is causing the providers to collude with client and ends up billing wrong diagnoses, drugs and even overpriced services. There was more scrutiny of claims to determine viability before introduction of the Biometric system in the insurance industry. Insurers should understand that in as much as the system might have reduced cost of operations and improved business processes the fraudsters have also found easier ways of making money from the same.

The study found that positive correlation exists between medical insurance fraud losses and usage of biometric technology. The coefficient of determination (R squared) indicated that the two independent variables that were studied, explained 14.6.1% of the relationship between biometric utilization in claims authentication and value of fraud cases reported in Insurers offering medical underwriting services in Kenya.

5.3 Conclusion

The fig 4.2 shows that a maximum of Kes.13.4 Billion worth of medical premiums was written in that period and a minimum of 0, this was due to new emerging insurance companies and also mergers example Real Insurance was absorbed by Britam in 2015. The value of claims reported in the period was as a high as Kes.12.6 Billion. This shows that claim ratios are still very high which is expected according to reported released by Insurance Regulatory Authority 2015. Insurers are incurring huge losses due to increased medical claims which can be attributed to rising cases of fraud in the industry. A maximum value of Kes.7 Million worth of fraud cases was reported in the same period.

It can therefore be concluded that there is a usage of biometric technology has not been effective to curb fraud losses in medical insurance firms since the study shows that the value of fraud cases reported significantly increases with the gross written premiums on biometric technology and claims authenticated via the same between 2013 and 2014. As technology develops fraudster tactics become more advanced and complicated which has led to other forms of fraud, including internal fraud, money laundering and cyber fraud which can't be prevented by use of biometric technology. However, it was found that biometric technology has enhanced really enhanced service delivery within the medical insurance sector especially by way of managing benefits.

It can also be concluded that there are other factors which affect the medical insurance fraud like, strong internal control systems, existence of internal and external audit functions, and strong internal control systems. The coefficient of determination (R squared) at 92.1% and F' statistics at 192.67 clearly indicated that that the model was valid and fit with the current set of independent variables.

5.4 Limitations of the Study

A number of challenges were experienced in the research. Data was not easily available. The researcher relied on primary data where respondents were from insurance companies and Insurance Investigation Unit. Most respondents were very reluctant to give information as they thought the report could tarnish their company reputation or the report could be used by fraudster to maximize on their weak areas. The researcher addressed this issue by using the introduction letter from the university.

The second limitation that was encountered is that it was noted that biometric technology has not been in use for a long period although the data points were sufficient. This means the same research should also be done in future to find out if there is any change in terms of findings from the current study. Also technology is dynamic which implies that some new features are likely to be developed that can enhance the effectiveness of the biometric technology.

There was also delay of getting feedback from the respondents. This is because the respondents needed some approval from the senior managers to give the information. The researcher addressed this by booking appointments with senior managers. Explanation also was given to the senior managers on why the study was important not only ot insurers but also the members as they will get to understand the importance of biometric technology as applied in authentication of individuals.

5.5 Recommendation for Further Research

From the findings and looking at the coefficients results in table 4.5 the gross written premiums is not significant, p=0.36, but the coefficient is negative -0.009 which would indicate that larger amount of premium is related to lower value of fraud cases reported. This shows that biometric technology has been effective to some extent in managing premiums but a study focusing only on the how biometric technology has been effective and to what extent it has been effective should be carried out.

Various stakeholders in the medical insurance industry should carry out research on how well fraud losses can be minimized. This should focus on the internal control systems and other information and communications systems employed by medical insurance firms to curb fraud. From the study that fraud can emanate at any point of insurance life cycle like even during the calculation of premiums where fraudsters attempt to interfere in with the calculation of premiums that should be paid by members. In other words the insured colludes with the underwriter and ends up paying lower premiums than expected

The researcher also recommends a similar research i.e. effectiveness of utilization of biometric technology to curb fraud in Commercial Bank in Kenya. In the recent past, most banks have adopted the technology in authentication of payments and also in identification of clients instead of using photos. This has also greatly replaced the tokens that are used in online payment approvals. The same technology again has also been applied in the use of Automated Teller Machines (ATMs).

REFERENCES

Abiola, J. (2013). *The Impact of information communication technology on internal control's prevention and detection of fraud*. Retrieved on July 23, 2016 from De Montfort University Faculty of Business and Law www.dmu.ac.uk/ipactinf.html

Abdullahi R., Mansor N. & Nuhu M. S. (2015). Fraud Triangle Theory and Fraud Diamond Theory: Understanding the Convergent and Divergent for Future Research *European Journal of Accounting Auditing and Fiancé Research,* 7(28), 1-8.

Agarwal, G. K. & Medury, Y. (2013). Good Governance – A Tool to prevent Corporate Frauds: *International Journal of Commerce, Business and Management,* 12, 2319-2828.

Albrecht, W. S., Hill, N. C., & Albrecht, C. C. (2006). The ethics development model applied to declining ethics in accounting. *Australian Accounting Review, 16*(1).

Allaire, Y., & Firsirotu, M. 2003. *Corporate governance and performance: The Elusive link*, Retrieved on July 22, 2016 from University of Quebec. www.uque.com/ccper.html

Albrecht, W. S., Albrecht, C. & Albrecht, C. C. (2008). Current Trends in Fraud and its Detection: A Global Perspective. *Information Security Journal* 17(9).

Albrecht, W. S., Albrecht, C. C., Albrecht, C. O. & Zimbelman, M. F. (2009). *Fraud Examination*. Natorp Boulevard, USA: Southwestern Cengage Learning

American Institute of Certified Public Accountants (AICPA). (2004). *Forensic and litigation services committee and fraud task force.* Discussion Memorandum. Forensic Services Audits, and Corporate Governance: Bridging the Gap. New York, NY: AICPA

Angima, B. C., & Omondi, A. M. (2016). Nature of Fraud and Its Effects in the medical insurance sector Insurance Fraud. *DBA Africa Management Review* 6, 33-34.

Association of British Insurers (2012). *No hiding place*. London: Association of British Insurers. Retrieved on August 8, 2016. www.abi.org.uk/nohipla.html.jp

Association of Certified Fraud Examination (ACFE), (2014). *Report to the nations on occupational fraud and abuse.* Retrieved on August 19, 2016, from www.acfe.com/rttn/docs

Beasley, M.S. (1996). An empirical analysis of the relation between the board of director composition and financial statement fraud. *The Accounting Review* 71, 443-465.

Benjamin, J. (2001). Internal Control and Fraud Prevention: The Account's Perspective, *Accountancy News Publication*, 5(1).

Cameron, E.D. (1982). *Report of the independent auditor on an efficiency audit of the auditor general's office under the Audit Act 1901, 5 March*, AGPS, Canberra.; retrieved July 17, 2016 from http://catalogue.nla.gov.au/Record/1796535

Clarke, M. (1990). *Business crime: Its nature and control*. 3rd Edition Cambridge: Polity Press

Cooper R. D. and Schindler P. S. (2003). *Business research methods*. Eighth Edition. McGraw-Hill. New York.

COSTA, L., (2007) *A Model for authentication of biometric for web banking*. Retrieved on August 16, 2016 from http://www.scmagazineuk.com/biometrically-challenged-three-factor-authentication-systems-too-weak-for-web-banking/article/484575/

Cressey, D. R. (1953). *Other People's Money*. Montclair, NJ: Patterson Smith.

Derrig, R. A. (2002). Insurance Fraud. *Journal of Risk and Insurance* 69 (3), 271-287.

Ernst and Young, (2011). *Fraud in insurance is on the rise*. Fraud Investigation Advisory Services East Africa 1-5 retrieved on July 23, 2016, from www.ey.com/publication/finrfr/pdfdocs

Ernst and Young. (2009). *Detecting financial statement fraud: What every manager needs to know*. Fraud Investigation Advisory Services. UK. Retrieved: August 2, 2016 from http: www.ey.com/Publication/vwLUAssets/FIDSFI Detecting Financial Statement Fraud.pdf/$FILE/FIDSFI_ detectingFinanceStatementFraud.pdf.

Gill, K. (2001). *Insurance Fraud: Causes, Characteristics and Prevention*. PhD Thesis, University of Leicester. Retrieved from on July 30, 2016 www.le.ac.ke/thesis/pubilcationpdf

Goetz, B. (2011). *The Handbook of deviant behaviour*. Oxford: Routledge.

Hair, (2003). *Social research methods* Inc., West Hartford, CT.

Hart, G. & Moore, M. (1988). *A statistical Study of State Insurance Fraud Bureaus-A quantitative analysis-1995-2000* Washington, D.C. Coalition against Insurance Fraud.

Hooper, M. J,. & Pornelli, C. M. (2010). *Deterring and Detecting Financial Fraud: A Platform for Action.* Retrieved on July 25, 2016 http://www.thecaq.org/docs/reports-and-publications/deterring-and-detecting financial-reporting-fraud-aplatform-for-action.pdf?

Jain, A. K., Ross, A., & Prabhakar, S. (2004). *An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14*1. Retrieved August 16, http://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

Jain A.K., Ross A., & Pankanti S. (2006). *Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security 12*, http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainRossPankanti_BiometricsInfoSec_TIFS06.pdf

Kiragu, N. D., Gikiri. W. L., & Iminza, N.W (2015).Bank size and occupational fraud risk: empirical evidence from commercial banks in Kenya**.** *European Journal of Business Management, 2* , 189-404.

Kisaka G.N., (2012), *A fraud Investigative and Detective Framework in the Motor insurance industry: A Kenyan Perspective*. Retrieved on July 23, 2016 from Strathmore University Faculty of Business https://su-plus.strathmore.edu/handle/11071/3396

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. Second Revised Edition. New Age International Ltd. New Delhi.

Levi, M. (2008) *The Phantom Capitalists: The Organisation and Control of Long-Firm* Fraud. Revised Edition. Aldershot: Ashgate.

Lister, L. M. (2007). A Practical Approach to Fraud Risk: *Internal Auditors*. 6(61).

Liu, S. & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional*, 3(1), 27–32

Mazar, N., Amir, O. & Ariely, G. (2007). *The Dishonesty of Honest People; A theory Of Self-concept maintenance*, working paper, Massachusetts Institute of Technology

Mugenda, M. & Mugenda A.G., (1999). *Research Methods: Quantitative and Qualitative Approaches.* Acts Press. Nairobi. Kenya.

Monaghan, C.T., (1989) '*Comprehensive Auditing for Efficiency' in Selected Addresses on Public Sector Auditing, No. 5, AAO, Canberra* retrieved from on August, 16, 2016 from ro.uow.edu.au/cgi/viewcontent.cgi?article=1070&context=accfinwp

Ngalyuka, C., (2013), *The relationship between ICT Utilization and Fraud Losses in Commercial Banks in Kenya*. Retrieved on July 5, Univesity of Nairobi. http://chss.uonbi.ac.ke/sites/default/files/chss/Relationship%20between%20ICT%20and%20Fraud%20in%20Commercial%20Banks%20in%20Kenya.pdf

Price Waterhouse Coopers Kenya. (2011). *Global Economic Crime Survey: A Step Ahead Economic Crimes in Kenya.* Retrieved on August 5, 2016 from https://www.pwc.com/ke/.../**economic-crime**-in-**kenya**-2011.p

Rae, K., & Subramaniam, N. (2008), Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal*, 23(2), 104-124.

Rasha, K., & Andrew, H. (2012). The New Fraud Triangle, *Journal of Emerging Trends in Economics and Management Sciences,*3(3).

Ramsay, J. R, Louwers, J. T , Sinason, D. H. & Strawser (2007), *Auditing & Assurance services.* McGraw-Hill.

Ramaswamy, V, (2007). New Frontiers: Training Forensic Accountants within the Accounting Program. *Journal of College Teaching & Learning* 4(9)

Rittenberg L. E. Schwieger J. B. & Johnstone M. K. (2008), *Auditing, A Business risk approach*, McGraw-Hill

Saunders, M., Lewis P., & Thornhill, A (2009*). Research Methods for Business Students.* Fifth edition. Pearson Education Ltd. London.

Siddiqui, A. T. & Muntjir, M., (2013). *A study of Possible Biometric Solution to curb Frauds in ATM transactions* retrieved from http://www.academia.edu/5310274/A_Study_of_Possible_Biometric_Solution_To_Curb_Frauds_in_ATM_Transaction

Sifuna, Anazett Pacy (2012). "Disclose or Abstain: The Prohibition of Insider Trading on Trial". *Journal of International Banking Law and Regulation* 27 (9).

Singleton, A. J. & Singleton T. W. (2010*). Fraud Auditing and Forensic Accounting.* Fourth Edition. John Wiley & Sons, Inc

Sitienei, A. K. (2012). *Factors influencing credit card fraud in the banking sector in Kenya.* Retrieved on July 4, 2016 from university of Nairobi. http://erepository.uonbi.ac.ke:8080/xmlui/handle/123456789/6639

Smart Cards and Biometrics in Healthcare Identity Applications. (2012) Retrieved on July 15, 2016, from http://www.smartcardalliance.org/resources/pdf/smart-cards-and-biomerticshealthcare_051112.pdf

Tistarelli M. & Nixon M. (2009), *"Advances In Biometrics", Springer- Verlag Berlin Heidelberg ISBN 03029743.* Retrieved on July 10, 2016 from http://www.springer.com/us/book/9781846289200

Tummibi S & Falayi E (2013). *IT Security and E-Banking in Nigeria.*Wells, J. T. (2011). Corporate Fraud Handbook: Prevention and Detection: 3rd Edition: Hoboken, New Jersey: John Wiley & Sons Inc.

VIigliazzi, D (2006*). Biometric: measurements from secure. 2 ed. [S.l.]:* Visual Books retrieved on July 10,2016 from http://www.biometricsinstitute.org/pages/types-of-biometrics.html

Vona, I. W. (2008). *Fraud Risk Assessment: Building a Fraud Audit Programme: Hoboken,* New Jersey: John Wiley and Sons

Wada, F., Olumide, L. & Danquah P. (2012). Action speaks louder than words understanding cyber criminal behavior using criminological theories. *Journal of Internet Banking and Commerce, 17(1).*

Wolfe, D., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal,* 74 , 38-42.

APPENDICES

Appendix I: List of Insurance Companies Underwriting Medical Insurance

1 AAR Insurance Kenya

2 APA Insurance Company

3 British American Insurance Company

4 CIC General Insurance Company

5 First Assurance Company

6 GA Insurance Company

7 Gateway Insurance Company

8 Heritage Insurance Company

9 ICEA Lion General insurance

10 Jubilee Insurance Company

11 Kenindia Assurance Company

12 Madison Insurance Company

13 Pacis Insurance Company

14 Real Insurance Company

15 Resolution Health Insurance Company

16 Saham Assurance Company

17 Tausi Assurance Company

18 UAP Insurance Companies

Appendix II: Questionnaire-Insurance Industry

Please answer the below questions

1. Name of the Medical insurance firm you work for…………………………………….

2. Respondent’s position…………………………………………………………………

3. Number of years of service with the firm……………………………………………

4. Which key areas are biometric used in your company…………………………………...

5. What type of biometric technology are your members using? Please tick

   I) Finger print technology
   II) Voice recognition technology
   III) Iris recognition technology
   IV) Face recognition technology

6. Please indicate the Gross written premiums from Members on biometric technology (smart cards).

   2015……………….

   2014……………….

   2013……………….

7. Please indicate the value of claims authenticated by use of biometric technology (smart card).

   2015……………….

   2014……………….

   2013……………….

Appendix III: Introduction Letter to Respondents

UNIVERSITY OF NAIROBI

SCHOOL OF BUSINESS

Telephone: +254-2-318262
Telegrams: “Varsity”,
Telex: 22095 Varsity

Baranabas Gisairo
PO.Box 1412- 00502
Nairobi, Kenya

Dear Respondent,

Re: Request for participation in research work

I am a postgraduate student pursuing a Master of Science (Finance) degree at the University of Nairobi, School of business. It is only one of the requirement that student is supposed to do a management research project for them to graduate.

I am currently conducting a research on effectiveness for use of biometric technology to curb fraud in medical insurance firms in Kenya. The information is going only to be used for academic purpose and will be treated with utmost confidentiality.

Yours Faithfully

Baranabas Gisairo
MSC (Finance) Student, University of Nairobi.