FRAUD IN THE BANKING INDUSTRY: A CASE STUDY OF KENYA

SERAH AKELOLA

A thesis submitted in partial fulfilment of the
requirements of Nottingham Trent University
for the Degree of Doctor of Philosophy

JULY 2012

Acknowledgements

Several people have made valuable contributions towards my research work. I am truly indebted to them all for sparing their time to support my work. It is impossible for me to mention every person here by name. There are, however, some people that I would like to appreciate. I would like to express my thanks to my supervisory team, particularly my Director of Studies, Professor Paul Whysall, for his academic guidance, mentorship, constant support and encouragement during the research process. I would also like to thank Professor Paul Barnes and Dr. Jing Wang for their invaluable expertise, constructive criticisms and guidance. I appreciate the support given to me by all the administrative staff from the Graduate School of Nottingham Trent University.

Many thanks also to my employer, Daystar University for granting me study leave and for believing in my potential as an employee. I cannot forget all my colleagues in the School Of Business at Daystar University for their great support, constant communication and networking to make my data collection possible.

Special thanks to all the Bank representatives who participated in the survey and interviews. Without you I would not have been able to produce this thesis – thank you.

To my wonderful parents, I am deeply indebted to you. Thank you for teaching me the value of academic excellence and inspiring me never to give up. To all my siblings, your love, support and encouragement have been fantastic and I thank you all for taking pride in my work and life. Thank you to all my friends, who have been there for me throughout the research process. Finally, I thank the Almighty God who makes all things possible and in whom all things consist for His abundant peace, grace and strength.

Abstract

Fraud has become a worldwide problem that is not set to abate in the near future. It is eroding the profitability of organisations with devastating effects on firm solvency. This research aims to contribute to the knowledge and understanding of fraud in Kenya's financial institutions and focuses on the Kenyan banking industry, which includes forty three commercial banks of local, national, regional and international standing. The research conducted uses a theoretical framework based on the Fraud Triangle to analyse the incidence of fraud and the motivations of fraudsters. The research uses a sample of audit, fraud, security and other managers involved in fraud fighting from thirty banks across the industry to conduct a mixed qualitative and quantitative study based on a survey of sixty respondents and seventeen semi-structured interviews. The research found that fraud is considered to be a major problem within the Kenyan banking industry, although the relative size of frauds conducted was relatively small and unsophisticated. Fraud detection and prevention methods used in the industry were standard and no different from global standards. The fraud triangle worked effectively to predict the patterns of fraud described by respondents. However from this study it is argued that the Fraud Triangle is not as effective in explaining the collusive and predatory nature of the Kenyan bank fraudster. Internal and external factors involved in fraud in Kenya are also identified, including weak industry co-operation, inadequately trained police and prosecutors, ineffective justice systems, weak government regulatory frameworks, low or non-existent fraud budgets for detecting and preventing fraud, among others. International banks were ahead of local, national and regional banks in efforts to establish industry co-operation; availability of capital, human, technological and other resources; dedicated fraud departments and budgets. Unlike previous research and theories that have mainly focused on either the individual or environmental factors, this research suggests an integrated theoretical and conceptual approach to fraud.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

The world banking industry is integrated in ways that would have been unimaginable three decades ago, due to the process of globalization. Globalization, or the process of expanding and integrating markets, regulatory frameworks, and international institutions from country to country in order to create a more integrated world governance and economic framework, has of course been a process that has reached back into antiquity (Busch, 2009). The rapidly expanding pace of globalization, driven by factors such as establishment of the World Trade Organisation (WTO) and subsequent lowering of market and competition barriers, has led to increased capital mobility and increased ability of financial services agencies to meet the needs of individuals and companies around the world (Busch, 2009).

However, the increasing rate of globalization, combined with the expansion of technology and other factors, has also increased the rate of fraud and new fraud activities (Zagaris, 2010). These new fraud opportunities can often be extremely difficult to detect due to their technological sophistication; thus, banks can spend considerable resources attempting to identify frauds and combat them (Kranacher, Riley & Wells, 2010). Banks face challenges in identifying fraud and preventing fraud and these difficulties can often be exacerbated by the political, regulatory, and institutional frameworks that are in place. However, even in the case of significant regulatory support, the regulatory framework of a given country cannot be expected to stop or even necessarily significantly reduce the incidence of fraud in the banking industry (Hoffman, 2002). This research focuses on the occurrence of fraud in the Kenyan banking industry.

1.1 Background of the Problem

The Kenyan banking industry is regulated by the Central Bank of Kenya (CBK), which manages bank supervision and monetary policy in line with key economic objectives within Kenya (Central Bank of Kenya, 2011). The Central Bank of Kenya was established following independence in 1966, and was re-established in 1997 with a higher

level of autonomy to set monetary and fiscal policy; however, the bank is not as yet fully independent. The bank's core mandate for supervision includes review and revision of laws and policies related to banking as well as licensing and oversight of financial services and banking agencies operating within Kenya, including commercial and retail banks, microfinance agencies, mortgage agencies, insurance companies, and other companies (Bank Supervision Report, 2008). As of Dec 2010 the total number of banks registered in Kenya included 43 commercial banks, 126 foreign exchange bureaus, two representative offices of foreign banks, two microfinance institutions, and one mortgage finance company (Bank Supervision Report, 2010).

In terms of performance, the Kenyan banking system is currently doing very well compared to other regional banking sector industries. The aggregate balance sheet for the banking sector increased by 23.4% over 2010 (Central Bank, 2010c), representing a total growth of 320.8 billion Kenyan shillings (KES). 19.9% of this growth represented loans and advances, and there was also an increase in the bank's deposit base of 19.8% (a total growth of KES 210.6 billion) (Central Bank of Kenya, 2010c). Total capital available increased by 20.8% over the course of the year, while non-performing loans fell by 5.7% (or a total of KES 3.5 billion). The banking sector's highest growth was reflected in profitability, with banks registering an increase of 48.3% in pre-tax profits during 2010 (Central Bank of Kenya, 2010c). Overall, this represents a strong growth in the banking industry, largely driven by increasing lending and decreasing poorly performing loans as well as an increase in bank operational efficiency (Central Bank of Kenya, 2010c).

Fraud in the banking industry is not formally tracked by the Central Bank, and thus there is no information regarding how this affects bank profitability and operational capacity. Although fraud is one of the focuses of the Kenya Bankers Association (KBA), information is still only thinly available. This research seeks to fill that gap by examining fraud in the Kenyan banking industry and identifying ways in which the industry could improve its fraud handling.

1.2 Aim of the Research

The aim of this study is to determine the nature and characteristics of fraud in the banking sector in Kenya and assess how the banking industry prevents and manages fraud, and to assess external conditions that affect the outcomes of the banking sectors' efforts to combat fraud.

1.3 Research Questions

Specific research questions have also been established to accomplish the research objectives. The four research questions that are addressed include:

1. What are the characteristics of fraud in the Kenyan banking industry? *This research question is explored using quantitative research (Chapter 5).*
2. What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry? *This research question is also addressed by quantitative research (Chapter 5)*
3. How do banks approach fraud management? *This question is answered through a combination of quantitative survey and qualitative interviews (Chapters 5 and 6)*
4. Are there differences between the approaches to fraud management adopted by Kenyan and international banks? *This research question was addressed by comparing findings in the qualitative and quantitative research from Kenyan and international banks, in order to identify similarities and differences in response, as well as literature review-based analysis.*

1.4 Scope of the Research

The scope of this research is limited by industry participation, time, and geography. This scope was defined in order to provide a discrete subject for comparison and to determine the boundaries of what would and would not be discussed.

The financial services sector includes commercial and retail banks, insurance providers, investment management firms, and other firms that provide services dealing with the flow of money. The choice has been made in this research to limit participation to commercial

and retail banks only, because of the complexity of defining an amorphous financial services industry as compared to a discrete banking industry.

The second limitation is geographical classification. For the purpose of this discussion, local banks are those banks who are headquartered in Kenya and whose main operations occur throughout Kenya. National banks are those that have operations in Kenya but in which the government has substantial participation in. Regional banks are banks that have operations in Kenya in addition to operations in another country in East and Central Africa (Kenya, Uganda, Tanzania, Rwanda, Burundi, Sudan etc.) and/or any other African country. International banks are banks that have worldwide operations across the continents. The choice has also been made to constrain the sample to include only banks that are licensed to operate inside Kenya.

Finally, there is a temporal limitation of the scope of this research. The history of the Kenyan financial industry is rich, and there is considerable scope for historical discussion of its formation, regulation, changes, and status. However, the current context of fraud in the banking industry includes elements that have not been consistently present, including the use of information technology. There are also problems with collection of reliable historical data in areas such as fraud, where the majority of fraud goes undetected (Wells, 2004). Given this, the temporal scope of this research is constrained to only include commercial and retail banks that are licensed in Kenya at the time of the research. This does introduce some degree of survivorship bias; however, given availability of information there was no way to avoid this bias.

1.5 Rationale for the Research

As stated by Bologna and Lindquist (1995), fraud is no simple vice. Over the past few years fraud has grown both in size and complexity. The costs of fraud are increasing worldwide. Studies in the UK and the USA indicate that the loss due to fraud continues to increase every year (KPMG, 2008; ACFE, 2004; ACFE, 2008). In Kenya details of fraud losses are not readily available. However, the KPMG (2005) report on the African Fraud and Misconduct survey indicates that fraud is a major concern among African companies

and employees are the main perpetrators. Six per cent of the African Fraud and Misconduct survey respondents said they had lost US$170,000 or more to fraud in the year 2001, and most respondents said poor internal controls, theft and corruption were the main causes of fraud (KPMG, 2005).

The lack of knowledge regarding fraud is likely to become an issue for development in the near future. Sub-Saharan Africa is rapidly becoming a target for increasing foreign direct investment (FDI), particularly from countries such as China and India which have begun to operate significant international investments in Africa (Broadman & Isik, 2007). This expansion includes Kenya, which has been a target for FDI in areas such as energy generation as well as others (Broadman & Isik, 2007). Given this, the current research and its goal of providing information about the nature of fraud inherent in the Kenyan banking industry, as well as discussion of what the industry is doing to combat issues of fraud, will provide valuable information for international firms considering involvement in Kenya. This research can provide insights on how to improve Kenya's access to international investment funds.

1.6 Significance of the Research

The present research has significance for theory as well as for empirical application in the areas of business and policymaking. Theoretically, the application of well known theories of fraud, such as the Fraud Triangle (Cressey, 1973; Wells, 2004) to the Kenyan context will provide more information regarding whether these theories can be considered to be universal or whether they are contingent on cultural constructions. The Fraud Triangle Theory hypothesizes that fraud is likely to occur when an individual is faced with pressure from a non-shareable problem, an opportunity to commit the crime and a rationalization to justify the fraudulent act. The research can also be expected to debunk some of the claims that are made in the academic literature regarding the experience of fraud in the African context and its meaning. Given the application of existing theories as well as the addition of more information from the research regarding the Kenyan banking industry, this can be considered to be important research from this viewpoint.

There are also significant practical applications of this research. The Kenyan banking industry can use the information gained from this research to modify its practices in order to better combat fraud, as well as to identify areas that are working well. Comparison to international firms can also provide information regarding practices that may be effective for the Kenyan banking industry. Investors are major users of this information in a pragmatic fashion. One of the major factors in foreign investment is financial risk, or the risk involved in dealing with the financial systems of a given country (Broadman & Isik, 2007). However, some degree of financial risk is inherent in almost all financial systems. Understanding the degree of risk and the specific issues that will need to be overcome will be extremely important for investors to make an informed decision. Finally, there is expected to be significant information derived from this research that can be applied by Kenyan regulators and policymakers. Legal, regulatory and law enforcement institutions are a major source of support for fraud prevention initiatives, but they can also hamper fraud prevention initiatives if they are not formed or applied correctly. By highlighting the problems that banks experience within the Kenyan banking system, this research will provide information for regulators on how regulations and institutions can be improved in order to reduce the impact of fraud on the Kenyan economy. It will also inform the law enforcement and judicial systems about the nature and characteristics of fraud and how to best assist in fraud prevention, detection, investigation and deterrence. Given the paucity of academic research from local Kenyan writers this study will be useful to academics, professionals and students of business in Kenya.

1.7 Structure of the Thesis

The thesis research was conducted in two parts, a quantitative survey completed by bank representatives who are knowledgeable about issues of fraud in their banks and in the industry. Qualitative interviews were conducted with bank managers who also work in areas or departments that handle fraud issues. The structure of the thesis is presented as follows.

Chapter One contains an introduction to this study. It lays out the background of the study and the aims, objectives and research questions of the research at hand. This chapter also introduces the scope, rationale and significance of this study.

In Chapter Two the literature on fraud, fraud theories, the external and internal environments that affect fraud levels, the banking environment in Africa and other related aspects of fraud such as responses to fraud and local and international banking issues are reviewed so as to provide an understanding of the nature of fraud and the context within which fraud occurs. This includes discussion of theories of fraud and its determinants, as well as empirical literature that provide evidence for potential outcomes of the research. This chapter also considers literature support for a few hypotheses the tests and results of which are discussed later in Chapter 5.

Chapter Three, on *Contextualizing Kenya's Banking Industry*, provides historical, regulatory, legal, political, and economic and market information about Kenya's banking industry and its structure, expanding the information that is offered in the Background within this chapter (Section 1.2). This chapter also presents the conceptual framework for the study.

In Chapter Four, the *Research Methodology* chapter describes the mixed methods approach that was considered appropriate in conducting the primary research of this study. This chapter discusses the research philosophy as well as the practical considerations that were relevant to the research.

Chapter Five, the Q*uantitative Study – Results and Analysis*, presents the results of the quantitative survey that is conducted covering a total of 60 respondents from 35 banks. Discussion of the quantitative survey is primarily descriptive and exploratory in nature. However, a few hypotheses are formulated in order to shed further light on possible relationships existing in regard to prosecution outcomes, use of software protection, fraud detection approaches and size of the bank as determinants of the size of loss to fraud.

Chapter Six reports the *Qualitative Results* of the seventeen semi-structured interviews conducted. The purpose of this chapter is to determine the common themes emerging from the study. The main themes include issues relating to individual perpetrators like collusion and internal controls; themes relating to banks and the internal banking industry environment such as industry co-operation in information sharing, customer training and customer competition, internal controls, fraud budgets and deterrence; and external issues such as structural, institutional, ethical, legal and computer based challenges. This chapter highlights how the qualitative findings relate to the research questions and the conceptual framework.

Chapter Seven mainly discusses the findings detailed in Chapter Six. An integration of the qualitative and quantitative findings are discussed in order to triangulate an answer to the research questions, and then analysed from the perspective of the literature. The themes that emerged from Chapter Six are discussed further in light of the conceptual framework capturing the individual perpetrator, internal banking industry environment and the broader external environment.

In Chapter Eight, *Conclusions and Recommendations*, the main issues that emerge from the study are discussed. This chapter focuses on the theoretical and practical contributions made by this study. A summary of the main findings and arguments based on the research questions is given. Contributions made to knowledge, theory and literature as well as policy implications and recommendations are addressed in this chapter. Finally this last chapter discusses the limitations of the study in terms of its application to other areas of study.

Chapter 2

Literature Review

2.1 Introduction

This literature review constructs a theoretical framework regarding banking fraud and provides a discussion focused on the research questions. The goal of the literature review is multi-fold. First, in Section 2.2 it presents the background information required to understand the problem of fraud in the banking industry in a real-world context. It defines fraud in the context of this study and outlines the different types of fraud that are the main focus of this study. This section also highlights the increasing trend of predicting perpetrators of fraud through the art of profiling. Section 2.3 presents the theoretical underpinnings of the discussion that will be used for analysis and examination. It discusses the main fraud theory used in this study as well as other theories of fraud. The discussion about the fraud theories leads into a discussion on the external and internal environmental factors that affect the levels of fraud. Various issues regarding local and international banking are considered in Section 2.5 while Section 2.6 examines various responses to fraud. An overview of the banking environment in Africa is captured in Section 2.7 and Section 2.8 presents hypotheses that will be tested later in Chapter 5

2.2 Fraud

This section considers the definition of fraud and explains the types of fraud in the context of this study.

2.2.1 Defining Fraud

The term “fraud” is difficult to define as its legal definition varies from country to country. For example, in 1888 the U.S. Supreme Court deemed that fraud occurs when a defendant knowingly makes representation in regard to a material fact that is false and the complainant acts on this representation reasonably believing it to be true. In the UK, the Fraud Act (2006) defines fraud as being committed in three ways; by false representation, by failing to disclose information, and by abuse of position. Meanwhile as observed by the Federal Bureau of Investigation (FBI) in the United States fraud is an illegal act

which is characterized by deceit, concealment, or violation of trust and which does not necessarily depend upon the application or threat of physical force or violence. The FBI definition of fraud can be narrowed down to lying, stealing and cheating (Silverstone et al., 2012) which resonate with today's fraud schemes in banks that are technically sophisticated. These definitions show the varying views about what constitutes fraud.

Individuals and organisations commit fraud acts to obtain money, property, or services; to avoid the payment or loss of money or services; or to secure personal or business advantage (Silverstone and Sheetz, 2004). Fraud therefore covers criminal offences that involve the use of deception for personal gain at the detriment or loss of another person. It includes activities such as deception, theft, bribery, corruption, forgery, embezzlement, misappropriation, conspiracy, collusion, money laundering, extortion and concealment of material facts (Chartered Institute of Management Accountants, 2008; Theft Act, 1978; Fraud Act, 2006).

For this study, bank fraud therefore involves the fraudulent use of one's position within or outside of the bank for personal enrichment by deliberately misusing or misappropriating the bank's financial resources, assets or other properties held by the bank and obtaining funds from bank customers (depositors) through fraudulent representation.

Fraud can be classified into three primary groups: fraud that has been exposed and is publicly known; fraud that has been discovered by organisations but not made public yet; and fraud that has not been detected (Silverstone and Davia, 2005). Only around 20% of fraud belongs in the group of exposed fraud. Reasons advanced for this are: most fraud is discovered accidentally; independent auditors do not proactively audit to detect fraud; entities without internal staff cannot audit to detect fraud proactively; most internal auditors do not have adequate training or experience to detect fraud proactively; and most internal controls are inadequate to prevent fraud (Silverstone and Davia, 2005; Wells, 2004; Albrecht, 2004).

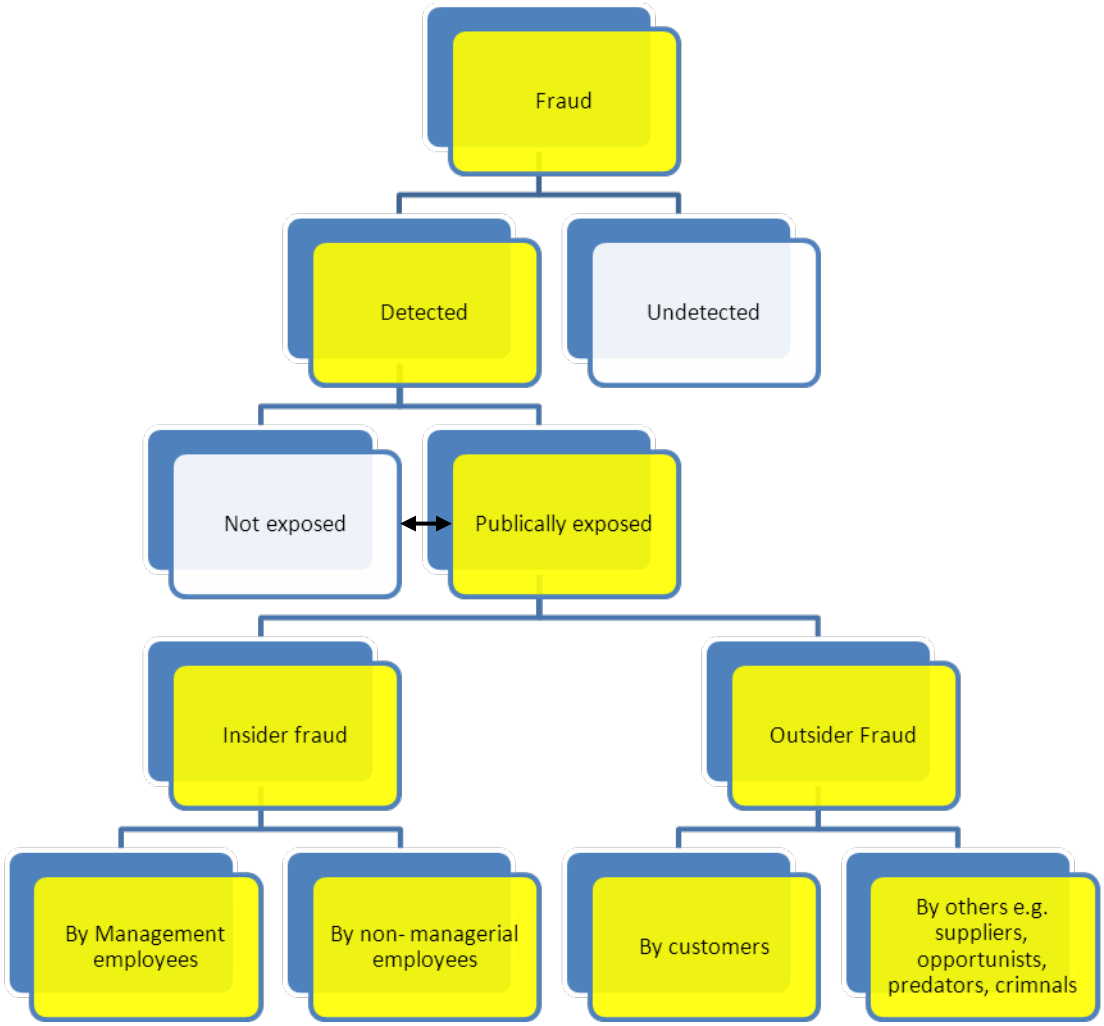


Figure 2.1 – Categorizing fraud

As shown in Figure 2.1 this study will mainly focus on detected fraud that has been publically exposed in the banking industry. However, due to the methods used in this research it is possible that there may be some evidence of fraud that has not yet been brought out in the public domain. Of the fraud that is publically exposed some is committed by insiders (i.e. managerial and non-managerial employees) while others are committed by outsiders such as customers, suppliers, agents, organised criminals, opportunists, and predators to mention a few.

Elliot and Willingham (1980) categorised fraud into management fraud and employee fraud. Management fraud is committed by managerial employees and consists of, but is not limited to: Financial Statement fraud, misrepresentation of material facts, misappropriation of assets, concealment of material facts, illegal acts, bribery, corruption and conflict of interest. Silverstone and Sheetz (2004) add that management fraud involves the manipulation of earnings reported in the financial statements prepared for shareholders and creditors. This type of fraud affects stock prices, management bonuses, availability and terms of debt financing.

On the other hand employee fraud, committed by non-managerial employees, consists of, but is not limited to: embezzlement, breach of fiduciary duties and theft of trade secrets of intellectual property (Elliot and Willingham, 1980). Additional items like pilferage, petty theft, false overtime claims, sick leave abuse, and use of company assets for their own benefit can also be viewed as fraud on the part of the employee, without forgetting bribery and corruption.

Insider fraud can also take on the definition advanced by the Association of Certified Fraud Examiners (ACFE, 2008, p.5) for occupational fraud that considers fraud to be “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organisation’s resources or assets.” The Association of Certified Fraud Examiners (2008) Report to the Nation (U.S.A) states that asset misappropriation, corruption and fraudulent financial statements form the three broad categories of occupational fraud. According to the ACFE (2006), asset misappropriation

in the U.S.A accounts for 80% of occupational fraud cases, corruption accounts for 13% while fraudulent financial statements account for 7% of the fraud cases. Though asset misappropriation was the most frequent occupational fraud committed, the losses on average were the lowest compared to the average losses due to corruption and fraudulent financial statements (ACFE, 2006).

In addition to management and employee fraud, there is customer fraud, such as false claim applications and fraudulent claims and the submission of false financial information on bank loan applications.

While the various actors (managerial, non-managerial employees, customers and other outsiders) are portrayed separately in Figure 2.1 they often work together in committing fraud through collusion as shown in Figure 2.2.

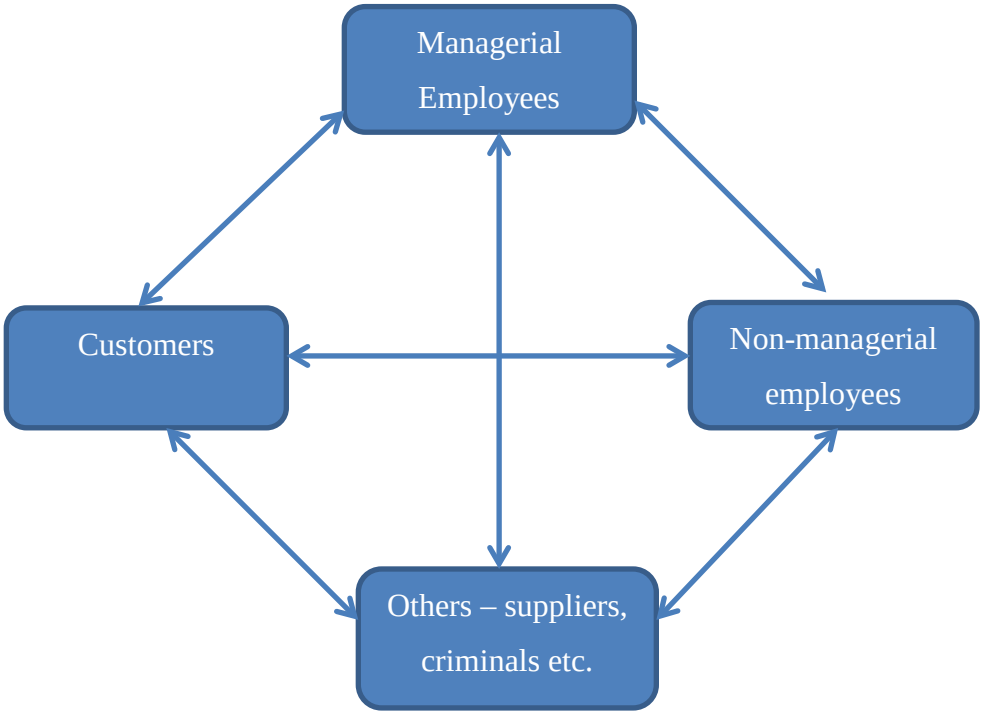


Figure 2.2 – Collusion among perpetrators

There are different combinations of possible collusion such as collusion within, between a manager and junior staff member; collusion externally, between customers and organized criminal groups or customers with agents or suppliers; and boundary spanning, collusion where an internal employee or manager works together with an external fraudster that may have particular skills to defraud the bank.

2.2.2 Types of Fraud

As explained in Section 2.2.1 above two distinct types of banking fraud can be identified. This section further discusses these two types of fraud in the bank. The first type of fraud is insider fraud, which is perpetrated by a member of the bank's staff or, but not endemic to the bank's control systems (Greenbaum & Thakor, 2007). This type of fraud may be typified at its extreme by the actions of Jerome Kerviel, the rogue trader that allegedly lost €4.9 billion in bad trading at the Société Générale investment bank in 2008 (Weiss, 2008). This type of fraud may also involve interaction with outside individuals, such as customers or other firms, who offer an incentive to the employee (such as a bribe or kickback) to facilitate the fraud (Mishkin, 2006). Control fraud is a type of insider fraud, but is executed at the highest levels of the company, with the company itself designed to hide and facilitate the fraudulent activities. It involves subversion of the corporate culture and control systems of the bank in order to perpetrate systemic fraud (Black, 2005b). This is the type of fraud that was perpetrated in many cases in the United States Savings and Loans (S&L) scandals of the 1980s (Black, 2005b). Finally, customers, suppliers, organised criminals and even ex-employees may perpetrate external fraud on the bank. This type of fraud is outsider fraud and it can result either from theft of personal data of legitimate customers of the bank or falsification of personal data in order to increase the likelihood of loans being made to customers that would not otherwise qualify (Mishkin, 2006).

2.2.2.1 Insider Fraud

The most important type of banking fraud is undoubtedly insider fraud, due to its prevalence and difficulty in detection and prevention. Research has indicated without

doubt that corruption of bank officials is a significant problem worldwide, according to analysis of the World Business Environment Survey (Beck et al., 2006). Insider fraud may be particularly expensive due to agency problems. Research indicates that the cost of exposed insider fraud is far more significant in terms of abnormal negative returns to shareholders than it is in terms of fines, fees and other losses assigned to the firm itself (Cloninger & Waller, 2000).

Insider fraud in the organisation can include many forms, including "embezzlement, insider trading, self-dealing, lying about facts, failing to disclose facts, corruption… cover-ups… [and] intentional misrepresentations in financial statements" (Zahra et al., 2007, p. 122). In banks it can also include the falsifying of loan documents, disclosure of bank or customer information which may result in fraudulent activity, theft of cash or cheques, misuse of bank assets and/or of one's position, identity theft, and electronic theft among others.

Insider fraud can also range from small acts (such as a small amount of embezzlement or falsification of a single document) to systemic internal fraud that affects all elements of the organisation. Although the most obvious reason to commit insider fraud is greed or demand for increased earnings, there are also a number of other reasons. Zahra et al. (2007) indicate that fraud committed within corporations is usually contrary to the usual assumption of societal pressures for consumption, as many if not most of the actors are paid well enough to meet their personal and societal-induced demands for consumption. Factors such as industry culture, investment horizons and payback periods, industry concentration, and environmental factors are likely to influence internal fraud. Top management overlooking or even encouraging fraudulent activities by others are often common (Razaee, 2005; Summers & Sweeney, 1998). Insider issues include board composition and responsibility for CEO accountability, management, attitudes and actions of the top management, and corporate culture traits such as emphasis on honesty (or in contrast creation of a culture of dishonesty) (Beasley, 1996; Crutchley et al., 2007; Dunn, 2004; Rezaee, 2005). One particular problem may be in cases where top management is very charismatic or connected, which can increase the tendency of the

organisation to follow the lead regarding corrupt practices (Zahra et al., 2007). Insider trading is commonly seen in cases where there is inappropriate screening or checking or family members or friends of those in the corporation (Brody, 2010). Brody (2010) argues that background checks alone are just one aspect of the employee selection and recruitment process and organisations also need to consider measures such as honesty and integrity testing. Insider trading charges are more common in business than investment activities, as these individuals may have more access to information and may be more likely to share it (Szockyj & Geis, 2002).

Although less common than 'garden-variety' insider fraud, control fraud is undoubtedly the most devastating type of insider fraud. Control frauds are crimes initiated by the Chief Executive Officer (CEO) or topmost managers of the organization. Control fraud, or modification of the internal systems that would otherwise detect fraud, was at the heart of the 1980s US Savings and Loan scandal (Black, 2005b). Control fraud is often driven by a motivation of "gambling for resurrection" (Pontell, 2005, p. 756), or attempting to mitigate or reverse the damage from previous losses before investors or regulators notice it. In this case accounting fraud is used, by the manipulation of financial statements, to deceive the creditors and shareholders of the company. Control fraud can also be driven by moral hazard, or the knowledge that if the fraud is discovered the cost will not be borne by the firm or perpetrators. Control frauds are some of the largest, most damaging and expensive types of fraud, because they have the potential to completely subvert a company, as well as the economy in general through introduction of a corrupt institutional system (Black, 2005a). One example of a control fraud is a Ponzi scheme, in which older investors are paid off with the money of newer investors in order to make it look like nothing is wrong (Black, 2005b).

Another common insider fraud that is more complex than simply embezzling money is earnings management, or "the alteration of firm's reported performance by insiders to either mislead some stakeholders or to influence contractual outcomes" (Shen & Chih, 2005, p. 2676). However, this approach primarily applies to public firms and occurs at the top level.

Another area where insider fraud may arise at the individual bank level is in poor quality bank loans. These loans may be offered to those whom the loan officer has a direct personal or business interest with, which may precipitate a conflict of interest, this inducing some degree of fraud. These loans may be constructed through a collusion of recipient and banker (Breuer, 2006). In some cases, bank inefficiency and insider conflict of interest may not be introduced through greed, but through a conflict of interest that lies in empathy with the customer population (Dixon, Ritchie, & Siwale, 2007). This may be important for the African case because conflicts may not be immediately apparent; for example, one case in a Zambian microfinance operation showed that loan officers struggled between the financial accountability requirements promoted by their corporate structure and the needs of the borrowers that were not always able to make payments in time. This demonstrates one of the problems with the current construction of banking fraud; specifically, that approaches to consumer fraud that are constructed in Western industrialized economies, which do not make significant use of microfinance or offer significant lending facilities to the poor, may not be appropriate in African banks that do offer this type of loans (Dixon, Ritchie, & Siwale, 2007). This is not just a problem due to the loss of income for the bank, but because in developing countries especially it may stymie development through funding inappropriate projects while leaving useful development projects unfunded (Barth et al., 2008).

2.2.2.2 External Fraud

Banking fraud may also be perpetrated from outside the bank, or external fraud. One common type of fraud is new account fraud, "which involves the criminal using a false identity, made-up or stolen, to open a new account, typically to obtain a credit card or loan" (Hartmann-Wendels, Mählmann, & Versen, 2009, p. 347). Another type of fraud is existing account fraud, where the criminal gains access to an existing account or set of accounts and uses them for fraudulent purposes. This can be seen through cases of hacking, phishing and scams. Existing account fraud is commonly easier to detect than new account fraud, as it becomes apparent from algorithmic detection rather than taking some time to become apparent, particularly if the fraudster maintains the account

legitimately for some time (Hartmann-Wendels et al., 2009). Identifying fraud is often done informally, which reduces the potential for a cost-benefit analysis to determine appropriate systems for detection (Canhoto & Backhouse, 2007).

In conclusion, this section has highlighted that fraud is a term that has varied legal definitions. This study focuses on fraud that has been detected and publically exposed. Two broad types of fraud have been identified: insider fraud and outsider fraud. Although fraud may be defined broadly as seen in the sections above, this study's scope does not encompass all potential forms of fraud that may occur. In this research, the focus is on forms of fraud that occur within the banking organisations and that are committed by management, employees, customers, and other people linked to the banks. However, this does not include the category of control fraud or management fraud, including systematic fraud associated with subversion of accounting systems and external fraud such as earnings management. These types of fraud were excluded due to the difficulty in detection and the likelihood that they would not be reported objectively by the respondents who are effectively an integral part of the control mechanisms of the firm.

2.3 Theories of Fraud

Over the past half a century, a number of fraud theories have emerged to explain the nature of fraud. The primary theory of fraud that will be used in this research is the fraud triangle theory posed by Cressey (1973). However, there are a number of additional theories that can be used to understand various aspects of fraud as well as the antecedents of fraud occurrences. This section first discusses the fraud triangle theory, and then briefly describes a number of other theoretical perspectives that can be used in examination of the research area.

2.3.1 Fraud Triangle theory

The most widely accepted fraud theory is that offered by Donald Cressey (1973), the criminologist who carried out a research on 200 embezzlers (trust violators) who had been incarcerated and held in various prisons in the US Midwest. Cresseys' final research statement was summed up as follows:

> "Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property." (Cressey, 1973, p30)

This hypothesis has popularly become known as the Fraud Triangle Theory. The legs' of the triangle respectively represent the individuals' pressure, opportunity and rationalization for committing fraud and is shown in Figure 2.3:

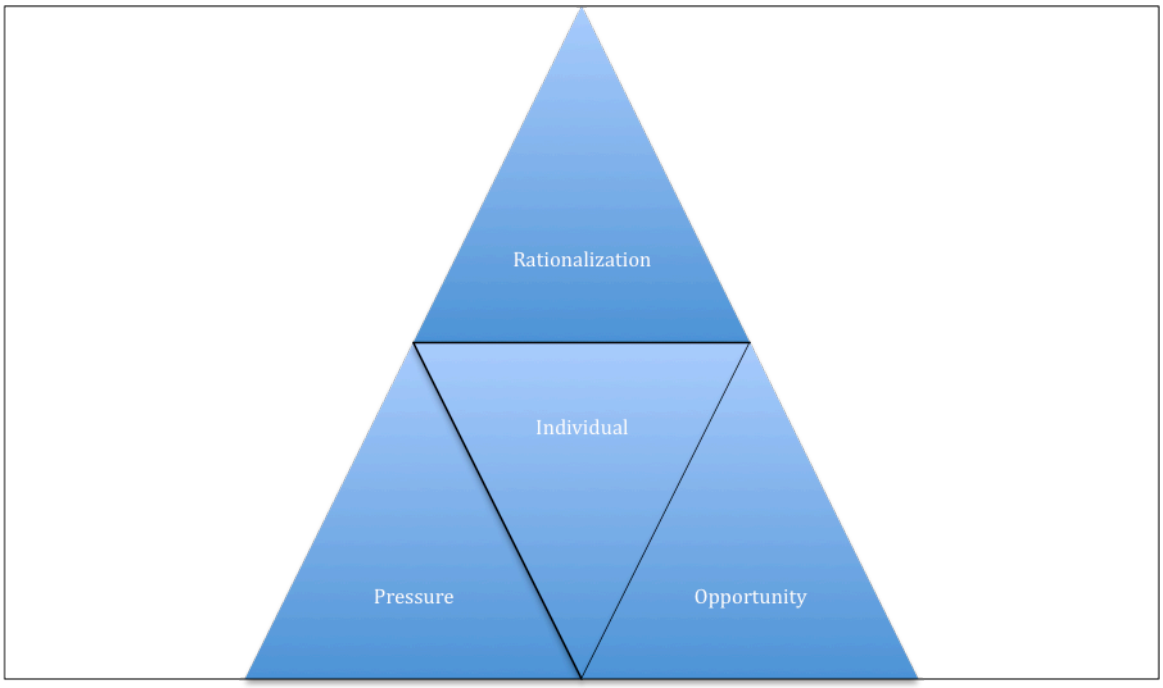


Figure 2.3: The Fraud Triangle
(Source: Adapted from Cressey, 1973)

The first factor, pressure on the employee, occurs due to "non-shareable" financial problems. Cressey (1973) identified fraud as being the outcome of problems that the individual perceived as being in some way non-sharable. He identified six types of non-sharable problems that were seen to lead to the potential for fraud within the individual. Figure 2.4 shows these types of problems. Cressey (1973) viewed the term "non-

shareable" as being relative, varying from person to person. Thus, what is non-shareable to one person may not be non-shareable to another. However, he concluded that non-shareable problems were concerned with status-seeking or status-maintaining activities. The six categories of non-shareable problems include violations of obligations, personal failures, business reversals, isolation from friends and associates, status gaining demands, and problems in the employer-employee relationship (Cressey, 1973).

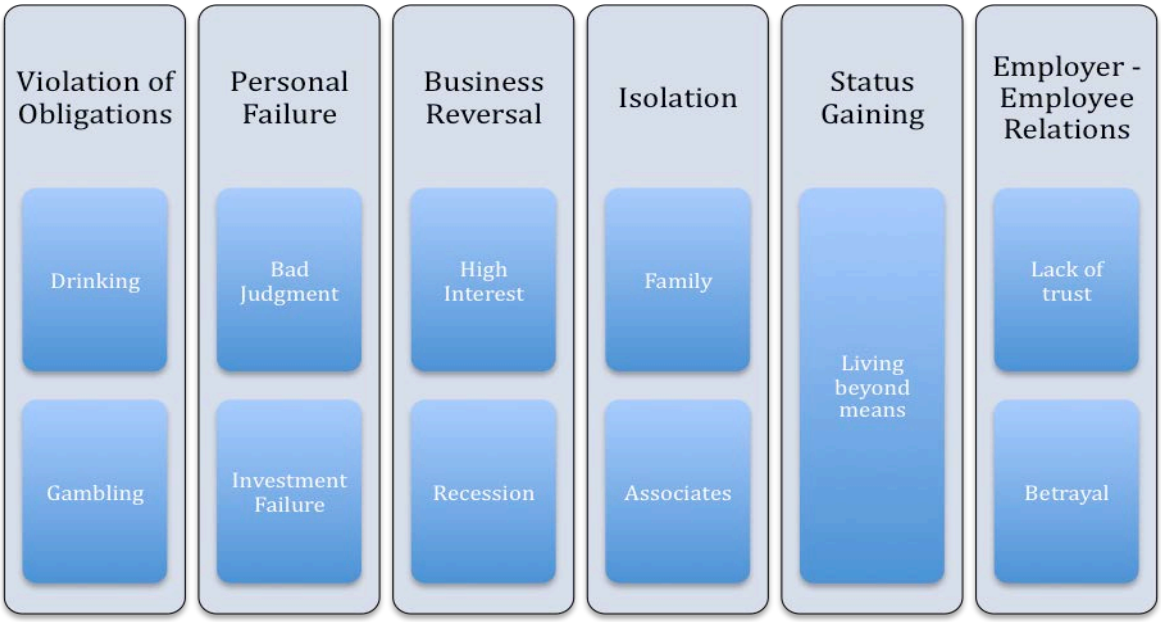


Figure 2.4: Six types of non-shareable problems
(Source: Adapted from Cressey, 1973)

The second factor of the Fraud Triangle is Opportunity. By itself the non-shareable problem will not lead an employee to commit fraud (Wells, 2005). The employee must also perceive that he/she has the opportunity to commit the crime without being caught. While the position of trust may provide an opportunity for the solution of a non-shareable financial problem, Cressey (1973) found that many trusted people did not at first see in their positions of trust the opportunities which such positions offer, and thus did not engage in fraud by using entrusted funds to solve their non-shareable problems. Making the connection between the non-shareable problem and the illegal solution is a product of the interrelated intellectual processes of knowing and rationalizing that the problem can be solved by violation of their position of trust. Rarely would a person in a position of trust not know, in a general way, that the position of trust can be violated, and therefore,

that an objective opportunity for trust violation exists. With respect to general information, Wells (2004) states that the very essence of an individual's fiduciary capacity implies that since the position is one of trust it is capable of being violated. Opportunities could present themselves in the form of poor internal controls, weak discipline policies or poor organisational ethics (Cressey, 1973; Wells, 2004).

The third factor to be considered is rationalization. The act of rationalization is not an after-thought that justifies the fraud, but it is the real reason(s) which the person has for acting in a fraudulent manner. Rationalization is, therefore, part of the motivation to commit fraud and is often abandoned after the criminal act has taken place (Wells, 2005). Cressey (1973) observed that a trusted person does not invent a new rationalization for his violation of trust, but rather he applies to his own situation a verbalization which has been made available to him by virtue of his having come in contact with a culture in which such verbalizations are present. The fraudulent individual acquires such verbalizations from other persons who have had prior experience with situations involving positions of trust and trust violation. This resonates the Differential Association theory earlier discussed (Sutherland, 1949) that suggests that an individual learns crime from their association with persons already exposed to it. Examples of such ideologies that seek to justify the crime are: "some of our most respectable citizens got their start in life by using other people's money temporarily"; "all people steal when they get in a tight spot"; "my intent is only to use money temporarily so I am 'borrowing', not 'stealing'; "I have been trying to live an honest life, but I have had nothing but troubles so 'to hell with it" (Cressey, 1973; pgs. 102-107, 110, 118, 124)

These cultural ideologies are contradictory to the theme that honesty is expected in all situations of trust. The individual uses such ideologies to adjust contradictory personal values in regard to criminality on the one hand and integrity, honesty and morality on the other. These rationalizations form excuses for the trusted person to violate the trust but are not sufficient in escaping legal prosecution. Employees who take organisation funds for their own purposes over a prolonged period of time have been known to consider themselves as borrowers rather than criminals. It is only when the rationalizations are

abandoned that the trust offender sees himself for what he is, a criminal (Cressey, 1973; Wells, 2005).

Cresset's Fraud Triangle has been used to explain the nature of fraudsters for many years. However, in concluding his research Cressey (1973) points out that the fraud triangle theory is limited in its practical use for prevention and detection of trust violation like fraud or for treatment of apprehended offenders. Wells (2005) has also echoed the same sentiment that the fraud theory triangle has had little application when it comes to fraud prevention. This theory is therefore open to revision.

One obvious critique of this model is that it describes antecedents that may be present in a large number of cases that do *not* result in fraud. Thus, the fraud triangle cannot be said to be predictive; rather it is a descriptive model that is best used in post hoc analysis (Day, 2010). Furthermore, the elements that are posed within this model cannot always be seen to be present; one example of this is many cases of executive fraud, in which there is no discernible non-shareable problem that must be solved by the fraud (Albrecht, Albrecht, & Albrecht, 2004). This means that even if the fraud triangle is used predictively, it cannot be used to fully model all cases, because some cases will fall outside this model. There is also a limitation in the existing research in that the majority of research is placed on issues of opportunity and putative motivation for the fraud. In contrast, elements of rationalization, cognitive capability to perform the fraud, and the incentive to commit fraud have been relatively poorly studied in the literature; thus, there are a number of assumptions that must be made about these areas (Holton, 2009). The reason for this lack of study may be due to a fundamental problem with the formulation of the rationalization construct; given that actually identifying the rationalization used by the individual at the time of the fraud is not possible and many individuals may engage in post hoc rationalization, there is no real way to identify the actual rationalization for the crime (Souse & Wright, 2008). This means that the majority of fraud research necessarily focuses on the development of opportunity and, sometimes, identification of fraud incentives, rather than rationalization.

2.3.2 Other Theories of Fraud

In addition to the fraud triangle theory, there are a number of other theories of fraud that can be identified within the literature. These range from the earliest theories such as differential association and cultural transmission theory, to domain-specific theories such as accounting fraud models, to specific observations that may be generalized to an area of fraud causation. This section discusses a number of theories of fraud causation that have emerged, specifically identifying the main points of the theories and discussing the uses and critiques of the theory.

2.3.2.1 Theory of Differential Association

Among the earliest theories was the "Theory of Differential Association", developed by Edwin Sutherland in the 1930's. Sutherland can be said to be the "Father of white-collar crime", being the pioneer researcher in the area of white-collar crime (Wells, 2005). He first researched on fraud committed by upper-class business executives either against shareholders or the public and he coined the term "white-collar crime" in 1939.

According to the Theory of Differential Association Sutherland (1949) suggested that crime is learned, just like any other subject. He believed that criminal behaviour occurred with other persons in a process of communication and hence criminality could not occur without the help of other people. Gaylord and Gallaher (1988) observe that Sutherland in departure from economic explanations, biological and pathological perspectives attributes crime to the social context of the individual. Sutherland (1949) viewed criminal behaviour as arising when an individual is exposed more to definitions favourable to violation of law than to definitions unfavourable to violation of law; hence criminal behaviour is a consequence of conflicting values. He theorised that the learning process consisted of two areas: the techniques to commit the crime and the attitudes, drives, rationalizations and motives of the criminal mind. Thus he found that organisations that have dishonest employees will eventually 'infect' a portion of honest ones and generally that honest employees will eventually have an influence on some of those who are dishonest (Sutherland, 1949; Wells, 2005). Today the Theory of Differential Associations is one of the most widely accepted theories of white-collar crime.

However, it is not without its critics. Akers (1996) criticised Sutherland's Differential Association theory based on the inaccurate assumption that Sutherland was suggesting that by simply interacting with criminals an individual would tend to criminal behaviour; but this was not what Sutherland proposed. Supporters of Sutherlands' Differential Association theory like Donald R. Cressey (Sutherland and Cressey, 1978) argue that some of these criticisms are misinterpretations on the part of the critics (Akers, 1996). Other criticisms emanate from the apparent inability of the theory to explain acts of deviance that are not necessarily learnt. Other authors argue that the theory cannot be measured empirically (Matsueda, 1988; Akers, 1996) due to the inability or difficulty in measuring and defining Sutherland's concept of "definitions" favourable and unfavourable to criminal behaviour. Sutherland did not clearly define which crimes were white-collar crimes as not all individuals in a position of trust hold a white-collar job, e.g. a vehicle mechanic.

Another criticism advanced is that Sutherland's theory represents a "cultural deviance" theory as it made incorrect presumptions about individual behaviour and the importance of culture in deviant behaviour (Matsueda, 1988). However Akers (1996) again argues that this criticism is yet another misinterpretation of Sutherland's theory. Laub (2006, p.1) argues that Sutherland's concept "was flawed because he embraced a sociological model of crime and in doing so adopted a form of sociological positivism." He further argues that Sutherland ignored key facts about crime that were contrary to his theoretical partialities.

Sutherland (1974, pg.82) summarized his own list of some of the criticisms levelled against his differential association theory, such as the theory: is defective as it omits consideration of free will; ignores the role of the victim; fails to explain the origin of crime; does not define terms such as "systematic" and "excess" clearly; ignore biological factors; can apply to non-criminals, and assumes all persons are equally exposed to criminal and anti-criminal behaviour patterns. In spite of criticisms brought forward against it, the Differential Association theory's contribution is strong and several

contemporary theorists in criminology and sociology have extended and expanded on Sutherlands' theory to explain criminal behaviour (Akers, 2004; Burgess and Akers, 1966; Bandura, 1997; Glaser, 1956)

2.3.2.2 Job dissatisfaction theory

Research by Hollinger and Clarke (1983) on 12,000 employees revealed that dissatisfaction motivated employees to commit fraud. When employees perceived that their jobs or working conditions were unfair, they were more likely to justify and commit fraud (Wells, 2005). However, this theory is difficult to prove due to the relative lack of information regarding employee theft in general; while it can be studied in its particulars, it is difficult to identify in general due to lack of reliable and widespread information about employee theft (Mustaine & Tewksbury, 2002). Furthermore, this model suffers from the same issues regarding motivation and rationalization as the Fraud Triangle theory.

2.3.2.3 The Fraud Scale

Steven Albrecht (Albrecht et al., 1983) also developed a fraud theory known as the "Fraud Scale" in the 1980s' that shared some of the fraud elements used by Cressey (1973) in explaining criminal behaviour. His theory suggests that three factors contribute to fraud: a situational pressure (like Cressey's financial pressure); a perceived opportunity to conceal the fraud; and, the level of the employees' personal integrity. The situational pressures are described as the immediate problems individuals experience within their environment. Opportunities to commit fraud may be created by individuals or by deficient or missing internal controls. Personal integrity refers to the personal code of ethical behaviour each person adopts.

As illustrated in Figure 2.5 Albrecht concluded that when situational pressures and perceived opportunities are high and personal integrity is low, occupational fraud is much more likely to occur than when the opposite is true (Albrecht, Howe and Romney, 1983). The main contribution made by the Fraud Scale model is the addition of the integrity dimension in explaining the occurrence of fraud. The integrity dimension was included as

a refinement to the rationalization concept suggested by Cressey (1973).

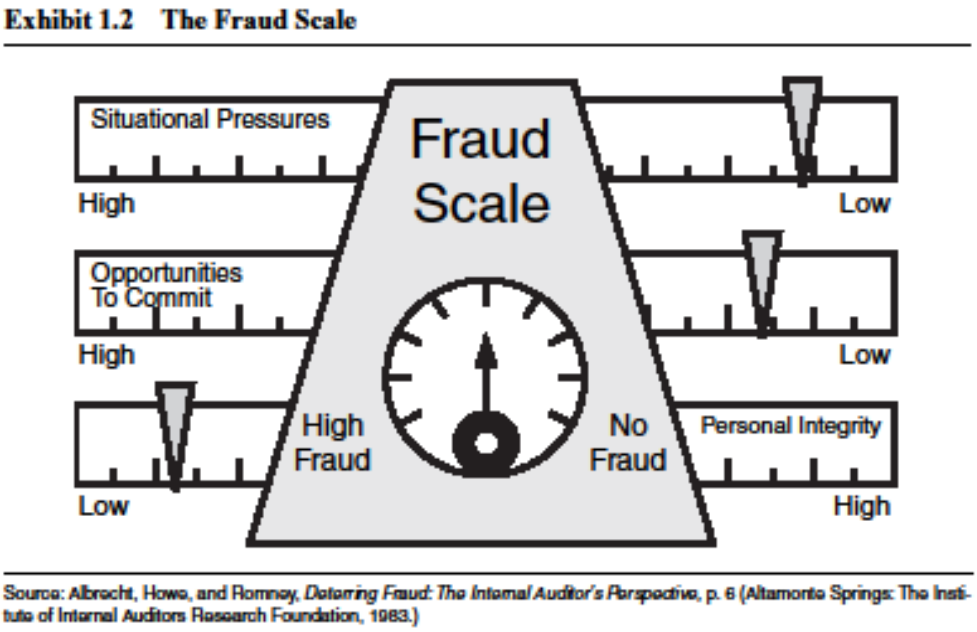


Figure 2.5: The Fraud Scale

2.3.2.4 The Fraud Diamond Theory

Wolfe and Hermanson (2004), building on the fraud triangle theory, theorized that another fourth element – capability of the offender – should be added to the fraud triangle to create what they term as the "Fraud Diamond". According to the fraud diamond theory, in order for fraud to be possible, other than having a motivation, opportunity and rationalization, the offender requires the capability of committing the crime, where capability may involve the technical knowledge, confidence etc. to execute and/or get away with the crime (Wolfe & Hermanson, 2004). The inclusion of cognitive capabilities and biases has helped to rectify some of the potential limitations of the fraud triangle; for example, one group of researchers uses cognitive heuristics to understand why in some cases managers may develop a rationalization to commit fraud, while others did not, based on individual cognitive biases and conditions (Anadarajan & Kleinman, 2011). This model has been little applied in the literature, but the addition of the fourth leg leads to social manipulation (Omar & Mohamad Din, 2010). Social manipulation, or the

involvement of others in the fraud through subterfuge or manipulation of emotions, social status, or other factors, is also often called social engineering. This form of manipulation allows the fraud perpetrator to involve others in the fraud, in order to use their access or skills to benefit the fraud perpetrator. Thus, this type of fraud may involve others as co-conspirators who are not fully cognizant of the nature of the fraud (or who may not know about it at all), but who are rather acting out of desire to help a co-worker or other acquaintance (Omar & Mohamad Din, 2010). This complicates the picture of the fraud offender, as one or more conspirators may *not* actually have the motivations associated with the formation of a fraud intention as described within the fraud triangle.

2.3.2.5 Eclectic theories

In addition to the formalized models presented above, there are a number of so-called eclectic theories of fraud, which present a combination of factors as being implicated in the formation of intention to commit fraud. This section presents a range of eclectic theories discussed within the literature and examines how these theories are tied to earlier theories.

2.3.2.5.1 Fraud in the Accounting Environment

The development of theories of fraud is on-going. An attempt to link fraud to the accounting environment was made by Riahi-Belkaoui and Picur (2000). They suggest a framework for fraud that can be used for identifying those situations most conducive to fraud in the accounting environment. The framework, shown in Figure 2.6 borrows from models and theories in the field of criminology such as the conflict and consensus approaches, the ecological theory, cultural transmission theory and anomie theories.

The conflict and consensus approaches hypothesize that laws develop from general public opinion reflecting the popular will of the society. The conflict approach suggests that laws are influenced and passed by interest groups to their benefit. This suggests that accounting interest groups give the impression that they are in control of problematic situations when they really are not. As a result the regulations that are enacted for checking fraudulent reporting and white-collar crime are weak. The conflict approach

also attributes fraud to a system of inequalities that condones certain types of aggressive behaviour that lead to crime and those engaging in fraud are reacting to life conditions of their own social class. Hence, the conflict model of crime proposes that the origins of fraudulent accounting practices may be connected to the political and economic development of a society (Carey, 1978, cited by Riahi-Belkaoui & Picur, 2000). In comparison, the consensus approach suggests that rather than emerging from and then exacerbating conflict between special interest groups, laws emerge from and then encourage cooperation between these groups, improving access to justice to all within the society (Riahi-Belkaoui & Picur, 2000). Under the consensus model, the origins of fraud are still connected to political and economic development, but rather than accounting interest groups being positioned as being weak, they are positioned as being actors in a consensus-building approach.

The ecological theory suggests that certain types of criminals are attracted to the fields of business and accounting. This theory blames the occurrence of corporate fraud, white-collar crimes and audit failures on the weak social organisation of accounting as a discipline and the failure of the general public to act effectively as an agent of social control by being indifferent to crime (Riahi-Belkaoui & Picur, 2000). Figure 2.6 shows the interactions between the accounting groups (who argue for private regulation), social institutions and inequality, social disorganization and elements of anomie, and the attraction of the criminal to the firm, which is perceived as a rich target, all of which together result in the various forms of white-collar crime. While this theory is highly complex and detailed, it has been little discussed within the literature and there has been little substantive involvement or application of the model. The application of this model may be limited in that it concerns itself with fraud mainly in the accounting environment rather than embracing a broader perspective of fraud. Thus, application of the model is complex and is likely to be difficult.

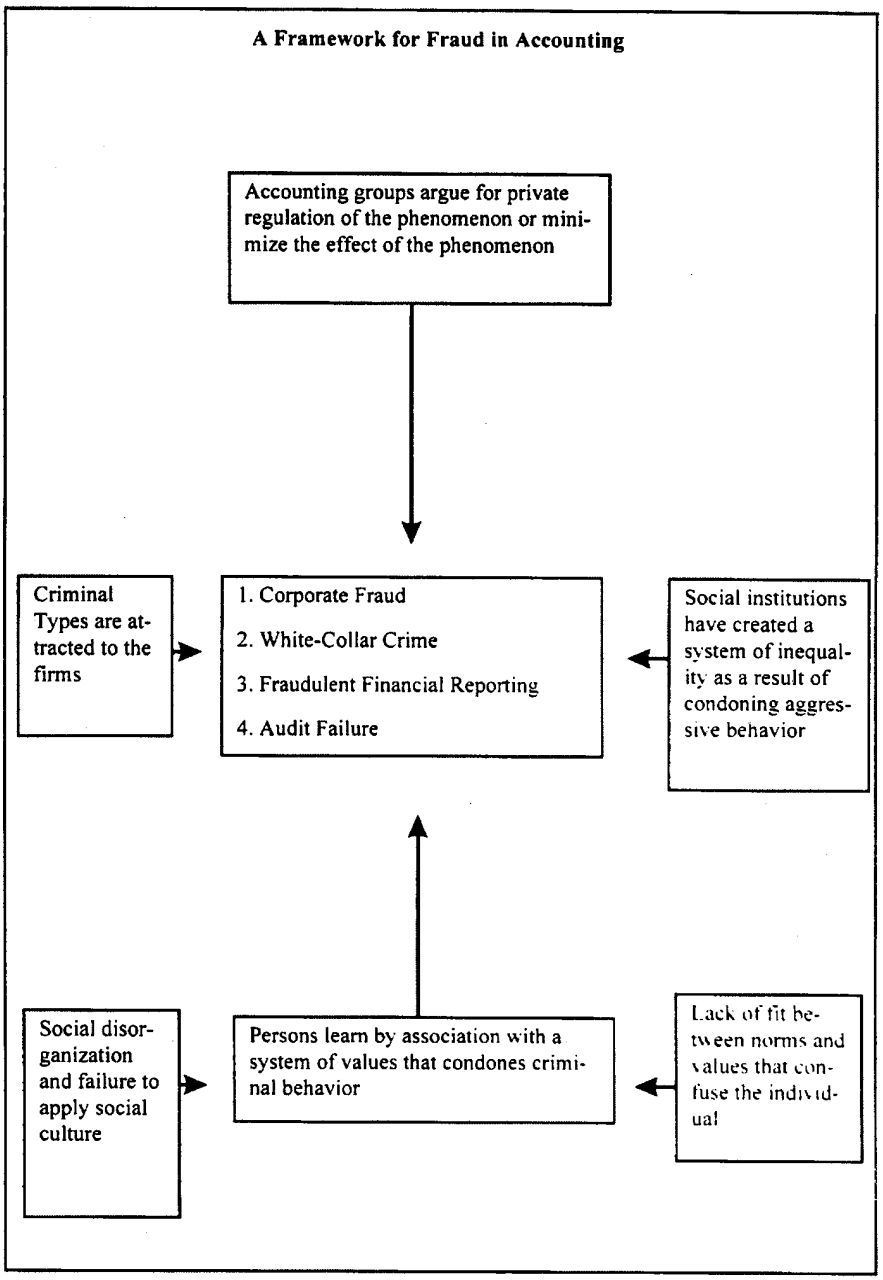


Figure 2.6: A framework for fraud in accounting.
(Source: Riahi-Belkaoui & Picur (2000), pg.41)

2.3.2.5.2 Cultural Transmission Theory

The Cultural Transmission theory is similar to the Differential Association theory put forward by Sutherland (1949) in which he suggested that criminal behaviour is learned. However, it differs from the Differential Association theory in that it presupposes the existence of a specific criminal culture, which is associated with people living in a specific area or within a specific ethnic group (Costello, 1997). The Cultural Transmission Theory assumes that criminals have been transmitted into a culture of crime by being socialized to accept specific values that condone crime. Therefore implying that fraudulent behaviour in accounting is learned. These sociological theories of crime emerged in the early 20th Century in order to explain the emergence of criminal groups in specific regions of a city, ethnic group, or class (Costello, 1997). However, this theory is much criticized due to its assumptions. In particular, it fails to take into account that those that are exposed to a so-called culture of crime are also exposed to mainstream culture, which affords individuals a number of different options and views as well (Cloward & Ohlin, 1966). In more explicit terms, the cultural transmission theory relates to a normative, middle-class moral system and positions everything outside this system as wrong or 'other' (Costello, 1997). This makes these models, according to Costello, both illogical and discriminatory; thus, this is not a useful model for understanding fraud in a given context.

2.3.2.5.3 Anomie Theories

Lastly, the Anomie theories concentrate on the confusion that ensues to an individual when there is a misfit between values and norms e.g. the dilemma between goals and the means to achieve it. In a bid to align the goals with the means an individual may adopt five types of solutions, including conformity, innovation (using illegitimate means to achieve success, as in accounting fraud), ritualism, retreatism, and rebellion (Durkheim, 1964; Merton, 1938; Merton, 1957). All these adaptations arise from the pressures of the society that accentuate economic success and the difficulty of achieving it. Thus the anomie theories involve the failure to match norms or values of ambition with the ability to realize the goals using illegitimate means (Durkheim, 1964; Merton, 1938; Merton,

1957). Anomie may seem to have a lack of application to the modern executive fraud case, but in fact evidence indicates that this is not so; instead, anomie may be perceived at the highest levels, and often poses a much more significant problem at these levels than at lower levels (Passas, 1990). However, one criticism of anomie theory is that the innovator and conformist categories are not mutually exclusive; in fact, many individuals that commit fraud may use both legitimate and illegitimate means to gain power (Murphy & Robinson, 2008). Thus, it is not as simple to just classify everyone into a single group based on their methods. There are also more fundamental theoretical critiques of the anomie model, especially that there are fundamental contradictions in the various specifications of the theory by Durkheim, Merton and others that have led to inconsistent and even opposing applications of the theory (Passas, 1999). Although Passas (1999) argues that there is continuity within the model, it is difficult to deny that there have been a number of different applications of this model.

2.3.2.6 Profiling of fraud offenders

Potential perpetrators of the types of fraud can be identified through the skill of profiling. With the advent of fraudulent scandals and corporate collapses (Enron, Tyco, World Com etc.) at the turn of this century, research in the field of fraud by accountants and auditors, as opposed to mostly criminologists, has grown. The emphasis of research has also shifted from just understanding criminal behaviour to looking at aspects of deterrence and prevention of fraud (Krambia-Kapardis, 2001; Smith, 2003). Profiling fraud involves classifying offenders in such a way that facilitates understanding criminal behaviour (Krambia, 2001).

Krambia (2001) carried out a study on 50 serious fraud cases in Australia. The study analysed the offences committed, the offender, the victim and the sentencing of the offenders by the courts of law. This research is a clear shift in the study of fraud as it introduces the aspect of prevention and deterrence. Weisburd (2001) also did a study based on 968 cases of offenders in the USA whose sample was based on an earlier study by Wheeler (1998). This research explored the criminal careers of white-collar offenders and identified three categories of offenders: those who commit crime as a result of a

crisis, those who commit crime due to greed and were exploiting an opportunity that had presented it-self and those who were pursuing a career in crime (chronic offenders). The profiling of offenders is useful in the prevention of fraud. Studies carried out by Krambia-Kapardis (2004), on developing a taxonomy based on 12 types of offenders, demonstrates that profiling fraud offenders can enhance fraud prevention and detection.

Later models such as the Eclectic Fraud Detection model suggested by Krambia-Kapardis (2002) still have at its centre the original contributions of the fraud triangle. One component part of this model is what is referred to as the ROP (rationalizations, opportunities and crime prone employee). This model has been tested using auditors and organisations in Australia and Cyprus. In Cyprus the model was used in a fraud victimization survey, where organisations were the victims of fraud, while in Australia auditors were involved in the study. In Australia and New Zealand a case study of 155 files of serious fraud (Smith, 2003) provided an indication of how serious fraud was committed, the characteristics of the offender and victims, the loss suffered, the judicial process and sentencing of offenders, motivations, rationalizations, mitigating factors and key risk factors behind the commission of the crimes (Smith, 2003; Krambia-Kapardis, 2001). This study on serious fraud once again highlights the importance of fraud prevention and deterrence. However, it is worthwhile to note that assessing the behavioural aspects of fraud in looking at the motivations, opportunities and rationalizations still remains an integral part of improving fraud prevention and detection.

More recently in Australia, attempts have been made at profiling fraud offenders (Steane and Cockerell, 2005). With the assistance of case studies and the Analysis Led Fraud Assessment (ALFA) Technique, they suggest that there are three components that cause fraudulent behaviour, namely: motivation, opportunity and a suitable target, and that in combination with these three fraud indicators, fraud methods and fraud consequences play an important role. We can therefore conclude that recent studies are focusing more on fraud prevention and deterrence, but at the same time there is an attempt to combine this with the behavioural aspects of fraud offenders (Wolfe and Hermanson, 2004; Smith, 2003; Krambia-Kapardis, 2004). This study intends to look at both behavioural as well as

environmental aspects that contribute to fraudulent behaviour.

While fraud profiling offers a certain amount of promise for detecting fraud, there are a number of issues and problems that must be taken into account in this practice. First and most obvious is that simply fitting the proximal characteristics of the fraud triangle (or any other diagnostic device) does not imply that the individual will commit fraud, or even will consider it as a viable option for resolving their financial difficulties (Day, 2010). In other words simply having pressure created by a non-shareable problem, sufficient rationalization and the opportunity to commit a fraud does not mean that the individual will succumb to the pressure. There are also issues with interpretation of profiling, especially with inferences from the individual's psychological state (if it can be determined in any great detail) to the actions taken (Canter, 2004). Dorminey et al., (2010, p.18) supports this view stating that the fraud triangle "does not adequately explain the actions of pathological fraudsters: predators who are better organized, have better concealment schemes and are better at interacting with auditors and antifraud professionals." The predator only seeks opportunity and does not require the other two elements of the fraud triangle, pressure and rationalization to enhance their chances of committing a crime. The typical fraudster has been profiled as a person that is middle aged, well-educated, a good citizen holding a position of responsibility, a trusted worker and a first-time offender (Dorminey et al., 2010). This individual does not set out primarily to commit fraud. They gradually succumb to pressure and are referred to as the "accidental fraudster" by Kranacher et al (2011). Predators on the other hand set out immediately to devise fraud schemes. Krancher et al (2011) further add that the fraud triangle was created with the "accidental fraudster" in mind rather than the predator. However, an individual can move from exhibiting the characteristics of an accidental fraudster to taking on the nature of a predator if they (accidental fraudster) are not caught in the initial stages of committing the fraud.

A further problem with the use of profiling is the issue of electronic evidence, which can often be more difficult to handle and interpret than physical evidence (Rogers, 2003). This may be particularly in the case of computer-based crimes, where the criminal may

have greater knowledge of the system than the investigator and thus be able to manipulate evidence. Furthermore, the majority of profiling (in general, as well as in fraud cases) is aimed not at identifying potential fraud perpetrators, but in identifying the characteristics of unknown perpetrators of crimes that have already been committed (Goodwill, Alison, & Beech, 2009). In effect this means that undetected perpetrators of fraud remain outside the scope of profiling.

Section 2.3 has examined various theories of fraud found from literature. The theory most significant to this study is the Fraud Triangle theory that is central to explaining an individual's fraudulent behaviour. Among the other theories, the Fraud diamond theoretically is similar to the Fraud Triangle Theory. The Eclectic theories emphasize the significance of environmental factors in affecting fraud levels. This section has also discussed the various theoretical models that consider the possibility of identifying potential fraud perpetrators through the art of profiling. More importantly the topics discussed above in Sections 2.2 and 2.3 (Fraud and the theories of Fraud) form the central part of the conceptual framework (Section 3.10, Figure 3.2). The next section examines more external and internal environmental factors that impact or contribute to increased levels of fraud.

2.4 External and Internal Environments impacting fraud

Even as environmental factors grow in importance, the general use of environmental information has not grown as much across the banking industry. This is mainly attributed to unavailability of accurate and comparable information that the banks can use on a shared basis (Murray, Kelly and Ganzi, 1997). Sharing information is important to an industry like banking as there is a tendency for banks to suffer the same type of frauds perpetrated by perhaps the same perpetrators. The size of the bank can influence formal information sharing (Berger et al., 2005). Historically in Kenya and Africa generally, bank instability and the absence or ineffectiveness of institutional boards at the period of early bank development has hindered the flow of information sharing (Neu et al., 2010) and encouraged fraud and corruption (Kane and Rice, 2001). Information sharing

therefore remains critical in bringing about co-operation and a concerted effort on the part of the banks in order to curb fraud and corruption.

There exists both an external and internal environment within and around the banking industry that impacts the levels of fraud. The internal environment includes the strengths and weaknesses of individual banks. On the other hand the external environment provides opportunities to the banking industry while at the same time it also poses threats. By taking advantage of the opportunities, banks in the industry can increase their profitability, market share and customer base, but this may inadvertently increase the risk of fraud

2.4.1 External Environment

The external environment of a bank consists of six main components, namely: the economic environment, technological environment, competition, the legal and regulatory sector, socio-cultural environment and customer sector (Popoola, 2000). These environments are discussed below.

2.4.1.1 Economic Environment

The economic environment comprises of economic factors such as exchange rates, inflation rates, interest rates, unemployment, economic growth rates, and stock markets among others (Popoola, 2000). Also related to the economic environment are the economic foundations of fraud. Economic foundations of fraud are based on agency problems, moral hazard, and the existence of incentives to commit or prevent fraud (Black, 2005b; Button, Johnston, & Frimpong, 2008; Crocker, 1998; Demirguc-Kunt & Detragiarche, 2005; Feldman, 2001; Krugman & Wells, 2006; Mayes, 2005). Each of these three elements, shown in Figure 2.7, offers explanations for why fraud occurs and why it remains persistent within the banking structure.

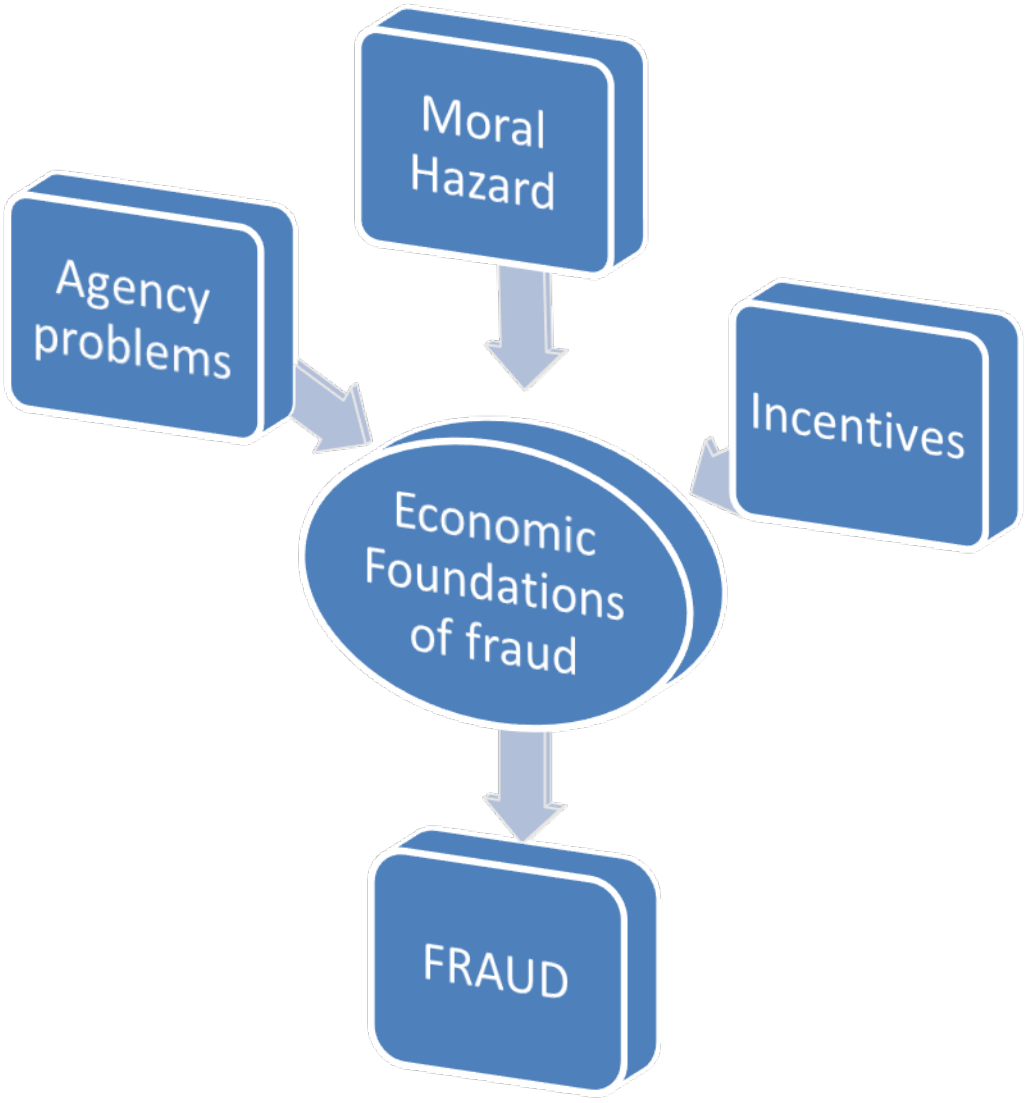


Figure 2.7: Economic Foundations of Fraud

An agency problem can be described simply as a situation in which an agent does not act in the interest of the principal or owner of the corporation, but instead in his or her own interest. The principal-agent relationship is a relationship in which there are two parties, the principal, normally the owners of the bank (who have ownership equity in a given asset and in whose interests the asset should be managed) and the agent (who acts to manage the asset for the principal). Because the agent has the main control of the asset and can control the information that is provided to the principal, it is possible that the

agent will be able to manipulate the management of the asset to his own advantage. In order to overcome this problem it is necessary to overcome the information asymmetry between agent and principal and to align the interests of the agent with the interests of the principal (Krugman & Wells, 2006; Stremitzer, 2005).

In the case of insider fraud, the individual that perpetrates the fraud is working against the interests of the principal (owners and stakeholders) of the corporation. However, it is important to note that simply eliminating agency problems could also be problematic. In this instance, an agency problem may be beneficial, as it could result in a whistle-blower alerting regulators to fraud by the owner against the interests of the owner (Black, 2005b).

Moral hazard is introduced into the banking system when the bank is no longer liable to pay for the full cost of any losses. Freed from this responsibility, the bank may act in ways that lead to a higher potential loss, including higher levels of risk taking in legitimate business as well as less effort placed toward reducing or eliminating fraud. This most commonly may occur through deposit insurance or another method for the government or the industry as a whole (Mayes, 2005). However, in the case of many developing countries, these structures have not yet been put into place; thus, consumers and customers, investors, owners, and the government will bear the cost of bank insolvency or failure (Mayes, 2005). Moral hazard may be introduced into the banking system is through depository insurance, which protects bank customers from some degree of losses in case of bank failure. Empirical evidence shows that deposit insurance increases the degree of instability in the banking system, and that the more extensive this insurance is, the higher the adverse effect is. Yet, deposit insurance is also necessary to build trust in the banking system (Demirguc-Kunt & Detragiarche, 2002). Thus, this is an element of moral hazard that is difficult to remove from the banking system. However, the issue of market discipline may fulfil some of the requirements of reduction of moral hazard, particularly in deregulated markets (Nier & Baumann, 2006). Market discipline refers to the conditions under which investors are willing to invest; simply, if effective conditions are not in place for investment banks will be negatively treated. Moral hazard

is key to discussions of banking fraud, particularly banking fraud associated with managers or others with some degree of agency in managing the firm, because moral hazard may promote a culture in which losses are not strongly tracked or accounted for, and in which the existence of depository insurance or other forms of protection can provide a rationalization for the fraud perpetrator to commit fraud (Mayes, 2005). Thus, moral hazard may promote the development of increased fraud.

Economic foundations of fraud are based primarily on incentives, including incentives to commit fraud and incentives to prevent or reduce fraud (Feldman, 2001). Feldman (2001) argues that fraud often remains undetected because of weak incentives for this detection. However, this is a significant issue, particularly in public policy, since this is a high economic cost that could be mitigated through the use of stronger incentives and organised programs for fraud prevention (Button et al., 2008). The use of incentives to prevent and detect fraud can be highly useful, for example in the use of optimal incentive policies, which identify the best incentive point to prevent fraud rather than create it (Crocker & Morgan, 1998). These economic issues are relevant to the specific creation of policies that will prevent fraud, as well as to the detection of fraud.

2.4.1.2 Technology Environment

The technological environment includes, most importantly, innovation of new products and services, research and development, new techniques and methods of service and increasingly significantly, information technologies which are relevant to the banking industry. Technological change has revolutionized the way financial data is stored, processed and analysed. At the same time it has improved the quality of banking services, risk management capabilities, led to reduction of banking costs and increased banks' lending capacity (Wilson et al., 2010). Increased globalization has made it easier for international banks to share information and technology (Claessens and Horen, 2008). In this study emphasis will be placed on the use of information technologies in banks for the perpetration, prevention and detection of fraud.

One of the major differences expected between local and international banks is the use of

information technology (IT). Research (Furst et al., 2002) shows that banks are likely to embrace new technologies like internet banking if they are part of a bank holding company (international banks and branches); are located in an urban area and mainly incur high fixed operating costs relative to their operating revenues. Therefore bank location, bank size and industry location have been found to be important factors in the adoption of internet banking technologies (Wilson et al., 2010).

The use of IT in banking auditing is a relatively recent development, only dating to the early 1990s (Shao, 1999). Early fraud detection systems worked on rule induction based on historical data, which compared typical and atypical data in specific users. By 1999, several larger banks and many small banks in the UK had adopted expert systems for fraud detection (Shao, 1999). Further refinements included the introduction of the use of case-based reasoning for new customer fraud, which applied multiple algorithms in order to compare the new customer with historical data (Wheeler & Aitkin, 2000). Other multiple algorithmic approaches were designed to work with skewed data as well, providing a highly cost-effective approach by integrating minority class training examples (Phua et al., 2004). The successful use of these algorithms was found to reduce even further the need for further manual investigation. Banks also began to use direct technologies to reduce existing customer fraud. By 2004, the chip and pin system was being tested as a means of prevention of card theft in the United Kingdom (Arnfield, 2004). The Meridien Card, first introduced by Meridien BIAO in Zambia in the early 1990s, was also an early experiment in shifting the fraud detection process toward the customer (Sardanis, 2007). This card acted as a physical identification card with the customer picture on the card as well as using smart card technology to prevent unauthorized access to the card (Sardanis, 2007).

Accounting and auditing systems are important for controlling and identifying inappropriate risk taking and potential fraud within the bank environment (Fernandez & Gonzales, 2005). Accounting and auditing information systems, if implemented properly, can maintain capital discipline and prevent circumvention of capital requirements. However, this effect is actually diminished by moral hazard resulting from deposit

insurance schedules as well as the size of the bank (Fernandez & Gonzales, 2005). This is relevant to Kenyan banking as the industry has had a history of bank failures arising from moral hazard, poor management, weak internal controls, undercapitalization and adverse selection (Brownridge, 1998; Brownridge, 1998b).

Some of the most common information systems-based methods of fraud detection today are based in statistics and machine learning (Bolton & Hand, 2002). These approaches vary widely in sophistication and technology in use, and can range from a simple historical comparison to complex neural networks creating behavioural models (Bolton & Hand, 2002). Many such techniques fall into the class known as data mining, or a process in which existing bodies of data within the organisation (up to and including all information flowing into and out of the organisation) is manipulated using machine-based processes in order to provide insight into various aspects of the data (Homazi & Giles, 2004). It does not necessarily provide certainties regarding fraud, but instead identifies potentially fraudulent occurrences from existing data (Phua et al., 2005). In Kenya the use of widespread information technology systems is not yet common in the banking industry. Kenyan banks are only now beginning to embrace fraud detection techniques such as data mining. Fraud investigation has remained largely manual and the use of smart cards and uniquely developed bank photo-cards have yet to be introduced (Gikandi and Bloor, 2010; Balancing Act, 2010).

The increasing cost of financial fraud has begun to move banks away from historical data analysis and toward the use of real-time data mining in order to detect and prevent fraud as, or preferably before, it happens (Edge & Sampaio, 2009). One such method is the construction of account signatures, in which new transactions are compared to a construction based on the user's previous activity (Edge & Sampaio, 2009). This statistical technique allows for detection and prevention of existing customer fraud in real time. The importance of techniques that utilise account signatures for fraud prevention purposes has been underplayed in Kenya over a number of years as it has been legally difficult to successfully prosecute fraud cases using electronic signatures as evidence in court cases. However, an amendment to the Kenya Communications Amendment Bill,

2008 (Government of Kenya, 2008) now gives Kenyan retail banks the same benefit enjoyed by their counterparts in the developed countries by making electronic records permissible in legal proceedings (Gikandi and Bloor, 2010). Thus there is expected to be growth in the use of such technology by Kenyan banks.

There is a growing use of neural networks and complex statistical techniques to detect both insider and outsider fraud in the banking environment (Paliwal & Kumar, 2009). These techniques require more sophisticated computing power and specialized development, but can be much more powerful (though more costly) (Paliwal & Kumar, 2009). The issue of the cost of technology is significant in the Kenyan banking industry. Due to lack of skilled manpower, most information technology systems currently in use in Kenya are externally procured. An international bank is believed to have procured a new information technology at the equivalent of USD50 million (Turana, 2011). Apart from the cost of the software banks have to contend with cost of procuring skilled expatriate manpower to implement and maintain the information technology systems (Turana, 2011). The cost and complexity of these systems, though potentially useful, places them out of the reach of many Kenyan banks, which continue to use older systems. Fraud prevention software is still not perfect. For example, the security API that accompanied the chip and pin cards deployed throughout the United Kingdom had significant flaws that prevented full security within this system, leaving customers open to some forms of fraud even though they are theoretically secure (Mannan & Van Oorschot, 2009).

Information technology can be used in the auditing process as well as in automated fraud detection procedures (Debreceny et al., 2005). The general class of computerized tools for auditing is known as Computer Assisted Auditing Techniques (CAATs) (Debreceny et al., 2005). One example of this is the use of generalized audit software (GAS), a type of software that allows the auditor to query the bank or business's databases and other programs in order to create specific views into the bank's financial position as well as detection of fraud (Debreceny et al., 2005). However, this is not always used. One study of international commercial banks in Singapore showed that external auditors did not use

GAS in any case, while internal auditors used GAS only as an exception to their usual work patterns and not as a general tool for use (Debreceny et al., 2005). A 2006 study indicated that digital analysis software, discovery sampling, and data mining were not commonly used in the organisation despite firms agreeing that they may be useful (Bierstaker et al., 2006). Thus, how useful this tool is can be debated.

Information technology is one of the most important tools in prevention and detection of fraud, and has grown substantially since its introduction in the 1990s. Early programs were based on historical analysis, but refinements including use of case-based reasoning for new customer fraud and other approaches including smart cards have dramatically improved the effectiveness of these systems. Accounting and auditing information systems allow for detection and prevention of fraud as well as implementation of capital discipline. Statistics and machine learning have further improved the effectiveness of systems, and real-time data mining is becoming increasingly important in banks attempting to lower the cost of fraud. Neural networks and complex statistical techniques require substantially more sophisticated computing software and hardware, and may be out of reach for local Kenyan banks. Although it is clear that the use of information technologies provides a significant competitive advantage for banks, the cost and technical complexity of these systems may place them out of reach for local banks. Thus, determining what type of information technology systems are in use and how effectively they are used will determine how Kenyan banks can compete in this regard with international banks.

2.4.1.3 Competition

Deregulation is one of the forces that has not only driven change in the banking industry, but has also served to remove barriers to competition. Studies by Zhao et al (2009; 2010) indicate that deregulatory measures geared at promoting competition resulted in increased risk taking in Indian banks. These studies also suggest that competition leads to increased risk taking in the banks.

Competitive pressure has driven banks and other financial institutions to opt for

diversification strategies (Wilson et al., 2010). The advent of new technologies has increased competition from inside and outside the banking industry. The use of mobile phone technologies in Africa, and specifically Kenya has led to new inter-sectoral competition for services once dominated by the banking industry.

2.4.1.4 Regulatory environment

This environment consists of political developments, policies, government legislation and regulations affecting bank operation. It also includes government action such as deregulation and the actions of law enforcement institutions, like the police, the courts and legal systems.

One of the driving forces of change in the banking industry is deregulation (Wilson et al., 2010). Deregulation, a driving force in the economic reforms on-going over the past thirty years, is one of the major enablers of banking fraud (Black, 2005b). Deregulation is important in the Kenyan context because of the on-going process of liberalization, privatization and other deregulation initiatives that have affected how corporations have operated (Barako et al., 2006). The experience of deregulation, despite its ideological assumption that industries will be self-policing, is that it increases the potential for fraud (Black, 2005b). Similarly, regulation has been shown to have an effect on the type and degree of fraud experienced. Changes in regulation and reporting requirements have brought about changes in the type of fraud commonly perpetrated in the banking industry. Green and Reinstein (2004) indicate that while the scale of fraud has declined, there are still about as many individual fraudulent incidents in the banking system, at least in the United States.

Law enforcement is a major structure of the institutional context that is needed for trade and effective market operations (Milgrom et al., 1990). However, law enforcement as an institution in Kenya is known to be weak and often ineffective in prosecution of criminals (Anderson, 2002). Thus, the state of law enforcement and the institutional capacity of the external environment will play a role in this study.

The provision of appropriate law enforcement protocols and specialists to combat fraud is a major social factor in preventing fraud (Button et al., 2007). In some countries, fraud and corruption specialists, or even complete specialist units, have emerged within the criminal justice system, as well as within specific regulatory organisations, in order to detect and prevent various types of fraud (Button et al., 2007). Many large banks maintain their own fraud investigation services. For example, a United Kingdom Serious Fraud Office (SFO) investigation found that the six largest banks in the United Kingdom had in-house investigation teams totalling approximately 2,500 investigators (Button et al., 2007). This is one way in which banks, as well as regulators, can reduce the potential for fraud. Identifying insider fraud can be much more difficult than external fraud, since insiders understand what systems are in place to detect them and have some degree of access and freedom in circumventing these systems (Porter, 2003). This difficulty is increased by the fact that many organisations take a reactive approach to identifying fraudulent activity, rather than a proactive approach to preventing it (Porter, 2003). In insider fraud cases, the use of law enforcement and forensic accounting may be far more useful than algorithmic or procedural methods (Porter, 2003). However, this does not mean that these methods should be ignored or discarded.

Although law enforcement is commonly regarded as the main instrument of the institution in preventing fraud, in the Kenyan context it may not be as effective, as Kenyan law enforcement institutions are relatively weak and often regarded as ineffective. In-house investigation organizations may provide some stopgap measures for banks attempting to prevent fraud, but the lack of support from dedicated and trained law enforcement officials may prevent the banks from effective fraud prevention.

Structural reasons for fraud in Kenya include slow judicial systems that do not allow for appropriate enforcement of legal rules; gaps in the legal framework intended to support the detection and prevention of fraud, and lack of independence in regulatory bodies (Omurgonulsen & Omurgonulsen, 2009). Additional factors include personal greed and social and ethical norms along with national culture (Black, 2005b). This also applies to issues like whistle-blowing (Black, 2005b).

2.4.1.5 The Customer

The customer in the context of this study is defined as the individuals or businesses that purchase or consume the services provided by the bank. A customer is an individual that does business with a bank through activities such as maintaining bank accounts, withdrawing or depositing money, transacting with debit and credit cards etc. The bank, in return for providing services to individuals and businesses, is able to earn some return from those provided with services

2.4.1.6 The Socio-cultural environment

The socio-cultural environment is a diverse mixture manifesting a range of social values, ethics, crime rates, age, gender, education, unemployment etc. In this study the socio-cultural environment will also include perceptions of the social problem of corruption, present in the business banking environment (Bakre, 2007; Transparency International, 2009) and generally acceptable business practice (Zahra, Priem, & Rasheed, 2007). Considering the impact that banking systems have on the development of an economy it is imperative that they operate efficiently. However, the banking systems in developing and transition countries do not always operate efficiently due to corruption. This problem of corruption is aggravated by the lack of adequate laws, prudential regulations, a lack of effective and efficient court systems and other appropriate institutions. Nevertheless objective courts and better law enforcement tend to curtail corruption (Barth et al., 2009). Barth (2009) found that increased competition and information sharing within the banking sector helps to reduce corruption in bank lending. Lending corruption was also found to be less prevalent in firms that were government or foreign owned and where the bank form of ownership was private and foreign.

2.4.1.7 The Political environment

The political environment is closely linked to the regulatory environment. This is because laws that govern and regulate businesses are determined by political processes. Some changes in government lead to a change in policies which can affect the business positively or negatively. The concept of political risk, that is the impact of political

change on businesses operations, includes wars and civil wars, riots, strikes, expropriation and other political risks (Buckley, 2004; Robbins & Coulter, 2012). In Kenya the banking industry has been affected by government interference through politicians' involvement in banks. Such interference has led to insider dealings some of which have been fraudulent in nature. This is discussed further in Chapter 3.

2.4.2 Internal Environment

Organizations use their strengths to mitigate their weaknesses. Through a SWOT analysis an organization can determine the resource capabilities and competencies that it possesses and which can give them a competitive advantage over their competitors (Robbins & Coulter, 2012). Considering the strengths and weaknesses of the banks is important in fraud prevention. Banks need to have adequate funds to meet the relatively high costs of fraud prevention. Having skilled human resources is also important and should be one of the strengths of a business. Developing efficient internal systems to prevent and detect fraud can help to reduce fraud. This section looks at some selected internal banking industry factors such as Corporate Governance, organizational characteristics, bank governance and risk taking and aspects of fraud prevention and detection.

2.4.2.1 Corporate Governance and Organisational Characteristics

Corporate Governance and organisational characteristics can influence the nature of fraud in a firm. Singleton and Singleton (2010) have shown that accounting transactions are influenced by factors like the type of industry, organisational culture, organisational strategy, culture and size of the organisation. Firms that are large in size find it relatively more challenging to have effective fraud control as their size impacts important fraud measures such as the segregation of duties. The size of the organisation is also a factor that determines the type and amount of fraud (value) committed as well as the control method adopted by the organisation.

Larger organisations are more difficult to control compared to smaller organisations due to various organisational complexities (Singleton & Singleton, 2010) and are therefore

susceptible to higher incidences of fraud. This is supported in a study conducted by Holmes et al (2000) where it was found that on average, perpetrators tended to victimise larger governmental entities (in terms of number of employees) as compared to relatively smaller private sector entities.

As the size of an organisation increases and the degree of supervision decreases, theft and fraud increases (Murphy, 1993). An empirical study by Barnes and Webb (2007) found that the larger the size of the organisation the more the susceptibility to theft and fraud. Sector or industry was not important, but corporate structure was, with more fraud occurring in Public Limited Companies (PLC's) and private companies. This seems to contradict the findings of Holmes et al (2000). However, it can be argued that the study by Barnes and Webb (2007) referred to type of organisation and did not specify whether these were large or small PLC's and Private Companies. In addition the study by Barnes and Webb (2007) found that monetary size of an individual fraud increased with organisational size.

Corporate governance serves as a protective measure against fraud by introducing elements such as internal controls, corporate culture and ethics, and oversight norms as well as enforcing specific laws regarding reporting and controls, thus reducing the potential for and incidence of fraud (Baucus and Near, 1991; Drew, Kelley and Kendrick, 2006; Macey & O'Hara, 2003; Rose-Ackerman, 2002; Sankar, 2003; Schein, 1996; Simons, 1995; Tadesse, 2006; Uzun, Szewczyk and Varma, 2004).

Corporate governance, or the management of the bank in order to meet the needs of the appropriate group of individuals, is at the foundation of the need for fraud prevention (Macey & O'Hara, 2003). The appropriate orientation of corporate governance varies depending on the business model in use. The Anglo-American model, used by banks derived from the American and English modes of doing business, focuses on a shareholder perspective (focusing on the rights and needs of equity owners in the bank). In contrast, the Franco-German model of corporate governance emphasizes the stakeholder perspective (focusing on the needs and rights of all stakeholders in the

business, such as customers, workers, and others) (Smith, 2003). However, in both cases fiduciary duties, or duties pertaining to the appropriate management of the bank, are owed to the group that is the focus of the corporate governance process (Kaler, 2003). This includes control of finances (including protection from internal theft), return of profits to the appropriate group, and reporting and records keeping requirements intended to protect the firm from regulatory repercussions or legal action (Winkler, 2004). One of the major problems of corporate governance is the separation of ownership and control, which introduces the possibility for an agency problem into the organisation (Macey & O'Hara, 2003).

The CLASS model of corporate governance provides one framework to understand corporate governance and reduction of risk within the banking structure (Drew, Kelley, & Kendrick, 2006). This framework – which incorporates elements of Culture, Leadership, Alignment, Systems, and Structure – is intended to promote the corporate culture and structure required to improve corporate governance and reduce the culture of risk-taking and the potential for corruption. This framework is shown in Figure 2.8. Organisational culture is influenced by leadership practices and systems. Culture is a perception and it represents ways of behaving and ways of understanding shared by a group of people. Hofstede (1980) defines culture as the collective programming of the mind which helps to distinguish members of a group of people from another. Organizational culture is described by Robbins and Coulter (2012, p.80) as “the shared values, principles, traditions, and ways of doing things that influence the way organizational members act” – briefly explained as “how things are done around here.” Mullins (1999, p.53) further defined organizational culture as “the collection of traditions, values, beliefs, policies, and attitudes that constitute a pervasive context for everything we do and think in an organization.” Leadership on the other hand is the art and process of influencing a group to achieve certain goals. Leadership is what leaders do (Robbins & Coulter, 2012)

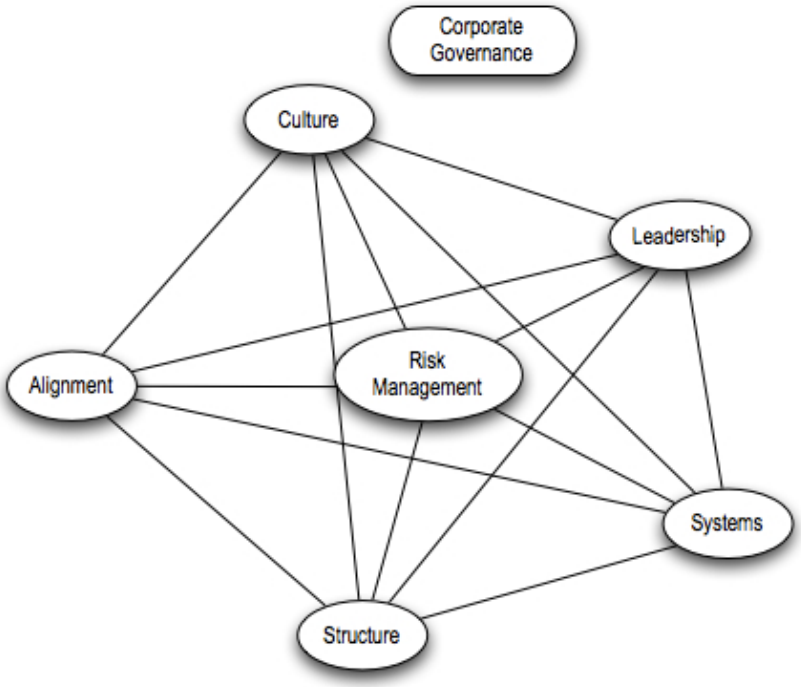


Figure 2.8: The CLASS model of corporate governance
(Source: Drew et al. 2006, p.129)

The purpose of alignment is to ensure that each element of the CLASS model works in harmony with other elements so that organisational culture reinforces leadership and systems reinforce the culture. All elements work together and no one element stands alone. Other studies have evidenced that organisational culture; leadership, systems and structures (Schein, 1996; Baucus and Near, 1991; Simons, 1995) cannot be easily separated. A study by Sankar (2003) reinforces the link between organisation culture and leadership while ensuring the alignment of culture with leadership.

Alignment is difficult to achieve as it involves a degree of conflict between the other four elements of the CLASS Model as alignment ensures each element is harmonized in relation to other elements. Labovitz (2005, as cited by Drew et al., 2006, Pg.133) defines alignment as “an optimal state in which people, key processes and strategies work in tandem.” He further noted that lack of alignment can lead to financial problems as well as problems in co-ordination and performance. Leadership styles need to be aligned with systems, culture and structure. A study by Uzun et al (2004) examined and found a

significant correlation between the composition and structure of the organisation boards and the incidence of corporate fraud. Corporate governance can also be effective in reducing losses from fraud. Disclosure, financial reporting, and financial disclosure regulations have been shown to reduce the level of financial crises in one study of 49 countries (Tadesse, 2006).

Although corporate governance is clearly highly relevant, implementing a Western model of corporate governance may prove to be problematic in Kenya, because of the differences between African and Western corporate governance models (McGee, 2008). The state of African corporate governance has traditionally been held to be inconsistent and prone to failure and fraud due to a kin-based, rather than a contractually based, system of obligations (McGee, 2008). However, evidence suggests that this may be changing rapidly due to both internal and external pressures, including a push for more external investment and external imposition of corporate governance rules from outside aid bodies (Rousseau, 2005). Thus, it is difficult to determine the precise nature of corporate governance that will be seen. This can best be considered under a plurality model rather than a dichotomous model, in which Kenya is considered to be a unique case rather than simply African or Western (Heugens & Otten, 2007).

There have also been some specific observations of corporate governance made regarding Kenya in comparison to the west. One short study found that Kenyan companies were approximately 29 days slower than American companies to report financial results (Muhoro & McGee, 2008). A second study found that voluntary disclosure norms in Kenyan companies, including positive effects from audit committees and negative effects from non-executive directors, were consistent with Western expectations regarding disclosure following privatization and reform of the Nairobi Stock Exchange (Barako et al., 2006).

There are a variety of perspectives on the role of corporate governance in fraud commission and prevention. The CLASS model of corporate governance reflects a number of elements of corporate governance that may affect fraud: culture, leadership,

alignment, systems and structure. Additional factors include size, specific business alignment, and corporate structure. Industry and sector, on the other hand, are less relevant in this area. However, care must be taken when applying findings from European firms to Kenya, as there are substantial differences between Kenyan corporate governance and Western styles of corporate governance. As such, the issue of corporate governance should be considered potentially important, but the existing findings should not be taken as directly transferable.

2.4.2.2 Bank Governance and Risk Taking

Corporate governance, as discussed in the section above, based on Western models may be complex to apply in developing countries, as in the Kenyan context (Rousseau, 2005). Understanding the characteristics of governance that are likely to lead to risk taking is important. The level of fraud inherent in the banking system may be related to the degree of risk taking involved in its business practices. In many cases insider fraud results from attempts to cover up excessive risk taking (Weiss, 2008). Excessive risk taking is an example of bad judgement that can lead to investment failure, a source of non-shareable problems as captured in Figure 2.4. Excessive risk taking also leads to moral hazard as already explained under Section 2.4.1.1. Theoretical evidence suggests that bank governance is dependent on the ownership structure of the bank (Laeven & Levine, 2009). Single ownership or highly consolidated ownership mitigates against aggressive risk-taking, while diversified ownership (such as public share-based equity ownership) creates pressure for aggressive risk-taking. This is due to the different level of potential loss for the owners in case of failed risk. Furthermore, owners and managers of banks may have a different view of risk taking, creating a conflict between these two areas; regulation also plays a role in reducing or mitigating the amount of risk taken by a given bank. As a result, empirical research has shown that the amount of risk taking in a bank is related to its ownership structure as well as to capital regulations, restrictions on non-financial activities, and deposit insurance regulation (Laeven & Levine, 2009). This demonstrates why bank governance and risk taking may be different from bank to bank, introducing a different level of risk within the bank.

2.4.2.3 Fraud Detection and Prevention Strategy

The use of effective fraud prevention techniques intended to prevent existing customer fraud particularly is important because without these techniques, it can be difficult to build trust between the bank and the customer, which can result in reduced ability to use Internet banking and increased customer churn (Suh & Han, 2002).

Types of fraud encountered in the banking environment include internal fraud and external fraud (Black, 2005b; Greenbaum & Thakor, 2007; Mishkin, 2006; Weiss, 2009). Fraud detection and prevention is at the heart of every fraud management system. Detection of fraud is highly complex, and a large percentage of fraud cases are actually detected externally (such as by the media or external auditors) or by accident (Dyck, Morse, & Zingales, 2007). However, approaches such as lifecycle monitoring and verification can be used to reduce the incidence of fraud overall (Potter, 2002; Porter, 2003; Wilhelm, 2004; Venkatraman & Delpachitra, 2008).

According to Wilhelm (2004) the fraud management lifecycle can be used to encapsulate the process of fraud prevention. This cycle consists of eight stages, including deterrence, prevention, detection, mitigation, analysis, policy, investigation, and prosecution (Wilhelm, 2004). The deterrence stage involves activities that hinder or discourage fraud through fear of consequences (Wilhelm, 2004; Webster, 1997, 1976, 1941). On the other hand prevention activities hinder, check, keep away or stop the fraudster from committing fraudulent activities. The detection stage uncovers existing or attempted fraud while mitigation includes activities designed to stop the continuation of the fraud e.g. blocking access to the bank account. The analysis stage seeks to determine the root cause of the fraud and the factors that led to the occurrence of the fraudulent activity. The policy stage is characterised by the creation, evaluation and communication of policies aimed at reducing fraud e.g. fixing limits to the authority to incur expenditure such as any transaction over £10,000 should be reported. The seventh stage of investigation brings together any evidence and information to curb further fraudulent activity, recover assets

or secure restitution and gather evidence necessary for the successful prosecution of the fraudsters. Many known frauds are not prosecuted due to concerns about the damage such prosecution could cause to the image and reputation of the organisation. The combination of internal factors (information technology, risk tolerance, fraud management philosophy etc.) and external factors (regulatory requirements, competitors, fraud methods etc.) all play a part in influencing fraud management. The complexity of fraud management increases with a dynamic and ever growing environment (Wilhem, 2004; Webster, 1997, 1976, 1941).

Bank verification has traditionally depended on the customer signature for verification of identity (Potter, 2002). However, the meaning of the signature has become increasingly complex as technology has changed and it has become increasingly easy to forge signatures, as well as to detect forgeries (Potter, 2002). A recent introduction to customer-side fraud prevention by banks is the use of biometric security (Venkatraman & Delpachitra, 2008). The use of this technology in banking is still relatively rare, although it is being piloted in the New Zealand Bio-Sec project, and poses considerable ethical and operational concerns in addition to being expensive (Venkatraman & Delpachitra, 2008). However, it represents a strong improvement on current methods of customer-side authentication.

Specific signs of potential fraud by insider employees that Porter (2003) identified included long hours, refusal to delegate, different behavioural patterns than expected, copying data, overriding controls, and relatively low levels of documentation. This suggests identifying these factors is crucially important for detecting fraud.

The rest of this section discusses auditing as a measure of fraud management. Also discussed here are the implications of recent regulatory requirements on whistle blowing and World Bank fraud prevention and detection rules. The goal of the discussion is to demonstrate how banks can prevent fraud as well as how fraud can be detected.

2.4.2.3.1 Auditing

Often a strong system of internal controls is the frontline defence that an organization can employ to prevent and detect fraud. The absence of internal controls does not always preclude the occurrence of fraud but it does leave potentially an open door for it to happen. Poor internal controls manifest themselves through: poor inventory control, lack of proper documentation and support for cash payments, lack of segregation of duties, ineffective or obsolete accounting software and the absence of independent verification (Doyle et al., 2007; Porter, 2003)

To prevent these failures, companies should conduct periodic risk assessments, lead by either internal or external auditing staff. The assessments should focus on high-risk areas, such as physical controls relating to high-dollar fixed assets, cash, marketable securities, payroll and inventory.

Specific questions should be raised during these assessments: Is there a policy of locking doors and filing cabinets after business hours? Does the company require the use of identification numbers and passwords, which are kept, secured and rotated on a regular basis? Does the company have a policy of mandatory vacations and job rotations? Does the company have at least one back-up copy of all data and software files stored at a secure off-site storage location? Does the company run background checks on new employees?

Internal and external auditing, or oversight by independent accounting professionals of the company's accounts and reports, is a major approach to fraud reduction (Wells, 2007). Evidence regarding auditing indicates that many companies actually desire audits even in the absence of regulation requiring it (Wallace, 2004). For example, following the 1996 relaxation of mandating auditing statements for private corporations in Canada, 73% of the companies that had previously been required to audit continued to do so even though it was no longer required (Wallace, 2004). Of the remaining 27%, many firms continued to use a review engagement rather than a formal audit (Wallace, 2004). This is consistent with agency and information theory, which indicate that auditing is an

important element in reducing agency problems and providing full information to owners (and not only to regulators).

The role of audit in fraud deterrence has become more pronounced in recent years. A report by the ACFE (2002) showed evidence from the USA that the audit function had a substantial impact on the size of the typical fraud. This report revealed that audited companies suffered less severe fraud losses compared to unaudited companies. This study further established that there were two reasons why fraud losses were less severe in audited companies; first the audit process itself, through routine procedures of examining documents, trend analysis and asset verification, was able to detect fraud and prevent it from happening or act as a future deterrent; secondly, awareness of and knowledge that auditors were watching was enough to discourage employees from committing fraud and served as an effective deterrent (ACFE, 2002). The use of management oversight can be an effective deterrent. However, the idea that someone is watching you does not always prevents fraud from happening but it does deter fraud to some degree as it increases the perception of likely detection. Internal audits therefore mainly play a detection and deterrence role (AICPA, 2012).

The role and impact of internal audit as a measure for detection and deterrence of fraud gained recognition with the implementation of the Sarbanes-Oxley Act in the USA. The Statement on Auditing Standards No. 99 (SAS 99) on Consideration of Fraud in a Financial Statement Audit, was the first major audit standard to be effected after the enactment of the Sarbanes-Oxley Act (AICPA, 2002). The importance of internal controls as a main fraud deterrence measure in the audit process is implied in both the Sarbanes Oxley Act and the SAS 99 which require management to evaluate and test internal controls and other anti-fraud programs to ensure they are effective. The role of internal audit is therefore to be responsible for evaluating, testing and examining the adequacy and the effectiveness of actions taken by the management in fulfilling their obligations. A person intent on committing fraud will be deterred if they think that the internal controls are strong enough to block their attempt. However, simply enforcing internal controls does not always prevent or deter fraud from occurring. This is more so

when one considers that often the same people who have oversight over the internal controls (management and employees) could potentially be the same ones involved in fraudulent activities, either individually or in collusion.

Historically companies have not considered fraud prevention as their main objective of internal control activities. Anti-fraud activities were mainly viewed as compliance activities rather than specific fraud concerns. However, today, internal control factors are quickly taking over compliance issues as the main drivers and initiators of antifraud activities (PricewaterhouseCoopers, 2004). No longer is fraud viewed at as an anomaly, or an infrequent failure of internal controls but after all the corporate scandals of the early 21st century (Enron, World Com etc.) it is seen as an important risk that can affect the entire life and reputation of the business. The role of audit in fraud deterrence is therefore shifting from being compliance driven to proactive detection and prevention of fraud embedded in audit function.

Taking into account that internal controls can deteriorate over time, either due to technological advances or human intervention (management overrides or collusion), other anti-fraud controls should be used (PricewaterhouseCoopers, 2004) to deter individuals from perpetrating fraud by sending out a message that the management are committed to fraud prevention and detection.

There is still no firm universal agreement on the responsibility of auditors for bringing fraud forward and the role of auditors to do so has not been clearly defined. For example, the auditors and the professional bodies responsible for setting the standards for the profession have varying opinions about the role of the auditor. Meanwhile the users of financial statements (normally the investors) expect that auditors will detect fraud as they (the users) do not always trust the management to detect fraud given that management can also act fraudulently. The auditors on the other hand know that it is not possible for to identify all fraud as their work is based on samples, meaning that some fraud would go undetected as they will not have the opportunity to look at every single transaction (Alleyne & Howard, 2005). Porter (1997) in a review of the historical role of the

auditor's duty to detect and report fraud noted a shift in auditing paradigm over the years. In the 1920's the primary objective of audit was to uncover or detect fraud (Porter, 1997). However, as the size and volume of transactions increased in the 1930's the auditors' role began to shift to that of designing and implementing appropriate internal control systems as well as the responsibility, towards the management, for detecting and preventing fraud. Two fundamental aspects of successful auditing are to ensure auditor's responsibility and auditor independence. In the 1960's, despite criticisms by the public about the reluctance of auditors to take on their role of fraud detection, auditors continued to downplay or minimize their role in fraud detection (Porter, 1997). With the advent of technology and the computer age in the 1980's, fraud incidences increased rapidly until the fall of large corporations like Enron caused the International Auditing Standards (IAS) to be revamped so as to re-emphasize the role of the auditor in fraud detection (IAS 135 and IAS 240). Nonetheless it is important to note that the IAS 200 still states that the primary objective of the audit is simply to form an opinion of the financial statements and not fraud prevention and detection activities of the organizations. Authors (Boynton et al., 2005; Oremade, 1988) are of the opinion that auditors should be more proactive in seeking to identify fraud in their regular audit activities.

However, auditor's responsibility brings with it the so-called expectations gap, in which there is a difference in views regarding whether or not the auditor is responsible for detecting and reporting fraud (Lin, 2004). The perception of auditor responsibility and independence varies depending on the cultural context as well. For example, Lin (2004) studied auditors in China, who indicated that self-regulation and less government involvement would be beneficial. However, other research has indicated that lack of government involvement can leave auditors vulnerable to undue influence by firm principals (Lee, Clarke, & Dean, 2008). Examination of the audit expectations gap in the Iranian context showed a gap that was largely consistent with, although not identical to, the situations in Saudi Arabia and China (Salehi & Azary, 2008). One study that took place in Barbados following the Enron scandal found that auditors view fraud detection as a management responsibility, while management viewed this as the responsibility of the auditor (Alleyne & Howard, 2005). This may vary depending on whether the

company has a sound internal auditing structure; in this case, there may be more interaction and cooperation between auditors and management, making fraud detection a group responsibility rather than an individual responsibility (Alleyne & Howard, 2005). The conflict between the view of management and the view of auditors regarding the responsibility of auditors in fraud detection also extended to Britain in the 1990s (Humphrey & Turley, 1993).

In some cases, the management of a company in addition to auditors are held formally responsible for fraud detection and prevention (Thomas & Gibson, 2003). This is particularly the case under the AICPA standards board, although this may not be consistent across accounting boards (Thomas & Gibson, 2003). There are still cases where conflict in consistency regarding auditor and manager views exists and that may result in lack of detection of the fraud; such conflict has clear implications for fraud detection and prevention because of the lack of consistent understanding of whose responsibility for preventing and detecting fraud.

One study found that despite pressure to enforce auditor responsibility for detecting fraud, the auditing profession resisted this change (Humphrey & Turley, 1993). Auditors often cannot correctly identify systematic or control fraud (Black, 2005b). However, since the Enron and WorldCom scandals of the early 2000s, auditors are expected to take a more active role in fraud detection in Britain and the United States (Evanoff & Kaufmann, 2005). The audit expectations gap continues to exist in many cultures (Haniffa & Hudaib, 2007). However, the specific contributory elements may vary from culture to culture. Porter (2007) suggests that education on the one hand can help in narrowing the auditor expectations gap while expanding the scope of audit to include additional auditor duties can mitigate the expectations gap. In so doing the public expectations and the auditors role can be more closely aligned, minimizing the gap.

Auditor expectations will affect the outcomes of auditing in some cases. One assumption commonly made by accountants is that internal controls are sufficient to reduce the potential for fraud; however, evidence shows that this is not the case, as fraud happens

even in organisations with strong internal controls (Wells, 2004). The efficacy of internal auditing as a control measure was tested by James (2003). The researcher found that the perceived independence of internal auditors was a major factor in perception of ability to detect fraud. Internal auditors that reported to senior management were seen as less likely to detect fraud than those that reported to the audit committee (James, 2003). This finding underscores the role of corporate governance in preventing internal fraud.

The ethical sensitivity of the auditor is also likely to play a role in whether the auditor will detect and bring to light potential fraud (Abdolmohammadi & Owhoso, 2000). In this research, it was shown that auditors that had knowledge of ethical actions by the corporation being audited were less likely to see fraud than those that did not have this information (Abdolmohammadi & Owhoso, 2000).

Accountants and auditors may be either complicit in fraud or the main perpetrator. This is an agency problem due to independent auditors being selected, hired and paid by the managers they are being paid to audit. This problem is not adequately dealt with in most auditing regulations, leaving auditor independence frequently in doubt (Gavious, 2007). A study of accounting and external auditing in Nigeria demonstrate that collusion with corrupted management has led to substantial losses through fraud over the past few decades. This has included both collusion through misstatement of accounts and, after companies have been placed in receivership, collusion with corrupt receivers as well (Bakre, 2007). Although the use of expatriate managers was used to reduce this, it is still a serious issue for the Institute of Chartered Accountants of Nigeria (ICAN) (Bakre, 2007). Another situation in which a small English accountancy firm was implicated in money laundering activities demonstrates this point (Mitchell & Sikka, 1996). In this case, Jackson & Co., a small accountancy firm, used a long series of Shell accounts in order to facilitate money laundering of funds embezzled by the chief accountant of AGIP (Africa) Ltd, an oil drilling company from Tunis. This fraud resulted in the loss of $10.5 million over the period of two years (1985 to 1987) (Mitchell & Sikka, 1996).

Fraud detection models are commonly used by auditors to detect fraud (Krambia-

Kapardis, 2002). A red-flags approach to fraud detection uses specific red flags to indicate that fraud may be occurring; for example, one common red flag is an employee who does not take his or her holidays (which can indicate that he or she is guarding evidence of fraud) (Krambia-Kapardis, 2002). However, a more sophisticated model is likely to be more effective, if this model can be defined appropriately.

One of the problems with external auditing as a means of protection from insider fraud and corruption is the relationship between the auditor and the senior manager (Lee, Clarke, & Dean, 2008). Analysis of previous insider fraud cases has shown that there is a pattern of auditors relying on senior managers for information and to be honest, but then rejecting their own responsibility to identify corruption within the reporting. Lee, Clarke and Dean (2008) explained this phenomenon as resulting from domination of the auditor by the senior management official; although the auditor identifies the fraud, he or she may be driven to not reveal it due to this personal interaction. In this case, the auditor may not deliberately hide the fraud, but may be taken in by lies or misdirection by the senior management of the firm. However, even if it is not intentional, this is one of the biggest problems with relying on auditing to detect fraud.

The use of effective fraud prevention techniques intended to prevent existing customer fraud particularly is important because without these techniques, it can be difficult to build trust between the bank and the customer, which can result in reduced ability to use internet banking and increased customer churn (Suh & Han, 2002).

Bank verification has traditionally depended on the customer signature for verification of identity (Potter, 2002). However, the meaning of the signature has become increasingly complex as technology has changed and it has become increasingly easy to forge signatures, as well as to detect forgeries (Potter, 2002). A recent introduction to customer-side fraud prevention by banks is the use of biometric security (Venkatraman & Delpachitra, 2008). The use of this technology in banking is still relatively rare, although it is being piloted in the New Zealand Bio-Sec project, and poses considerable ethical and operational concerns in addition to being expensive (Venkatraman & Delpachitra, 2008).

However, it represents a strong improvement on current methods of customer-side authentication.

2.4.2.3.2 Whistle blowers and regulatory requirements

Whistle blowing is traditionally a voluntary practice of individuals who observe something incorrect about a given auditing or accounting situation and bring it to the attention of auditors (Schmidt, 2005). However, there has also been a movement in recent years to introduce a regulatory requirement for whistle blowers, or to induce some regulatory compensation or incentive to blow the whistle (Schmidt, 2005). Schmidt (2005) found that a variety of measures in the US, UK and Germany have been identified and intended to enforce the obligation for whistle blowing. These include the US Sarbanes-Oxley (SOX) Act of 2002, the British Public Interest Disclosure Act (PIDA) of 1998, and a variety of special-purpose German regulations and case law (Schmidt, 2005). Although the specifics of each law vary, the ultimate intent is to influence the whistle blower to bring the irregularity to attention either through positive influence (monetary incentive) or negative influence (the potential to be prosecuted if it is found out) (Schmidt, 2005).

Whistle-blowers may face significant social pressures in African societies, however, which may mean that regardless of incentives, there may be a strong incidence of retaliation that will act as a negative incentive to engage in the disclosure activity (Domfeh & Bawole, 2011). There are also structural impediments to whistle blowing, such as elements of the African Union Convention on Preventing and Combating Corruption, which promotes a presumption of guilt that whistle-blowers must overcome (Schroth, 2005). A significant case of whistle-blowing relates to the infamous Kenyan Goldenberg Scandal (referred to in Chapter 3 Section 3.6). Another famous Kenyan whistle-blower, John Githingo, a journalist, also resigned his job and fled the country two years after unearthing evidence of corruption, fraud and graft at high levels of government in Kenya (Transparency International, 2007). These cases discourage the practice of whistle-blowing in Kenya. Even though some laws have been passed to protect the whistle-blower there is still lack of effective legal protection for whistle-

blowers in Kenya (Transparency International, 2007). Thus, whistleblowing, though it is considered to be valuable in a Western context, may not be effective in the Kenyan banking environment.

2.4.2.3.3 World Bank Fraud Detection and Prevention Rules

A major factor in the modernization of the Kenyan banking system has been the imposition of World Bank rules for development lending (McGee, 2008; Muhoro & McGee, 2008). Thus, World Bank rules are likely to be highly relevant for the development of fraud detection systems in the Kenyan bank. The World Bank has its own series of rules for fraud and corruption prevention and detection in World Bank projects. They include specific anticorruption policies intended to address corruption in the bidding and loan processes in general bank operations and case studies that highlight where and when fraud may be found (Aguilar et al., 2000). The guidelines also include a specific ethical guidance for bank staff intended to address problems of ethical practice by bank employees.

Section 2.4 has demonstrated the external environments (economic, technological, competition, regulatory, customer and socio-cultural) that exist outside the banking industry which influence fraud prevention and detection. This section has also reviewed aspects of the internal banking environment such as corporate governance and issues of fraud detection and prevention, and most importantly, the role of auditing. Banks, it emerges, must scan their external environment regularly to counter any threats and take advantage of opportunities while ensuring that they identify any internal strengths and weaknesses.

2.5 Issues in local and international banking

The section above has presented the immediate internal and external environmental elements that have an impact on fraud prevention and detection. This section focuses on selected issues in local and international banking. This includes discussion of international bank operations in Kenya, differences in corporate governance between

Kenyan and international firms, facilitators and consequences of bank fraud in Kenya.

2.5.1 International Banks in Kenya

International banks in Kenya have a long history and a relatively large market share of the retail banking population (Bank Supervision Report 2009). Previous findings in African banking indicate that international and regional banks have different approaches to fraud, one of the expected findings of this present research (Barako et al., 2006; McGee, 2008; Muhoro & McGee, 2008; Rousseau, 2005). Thus, asking the question of why international banks enter the market in the first place is relevant to understanding why differences between international and other banks is likely to emerge.

There are a number of reasons for entering the international market in addition to reasons of growth and profit. Some international banks may construct internal capital markets, allowing free flow of capital between international branches in order to reduce costs, grow credit facilities and provide competitive advantage (De Haas & Van Lelyveld, 2010). In some other cases, international banks may be drawn to developing countries with less regulatory pressures on banking as a means of effecting international market entry (Petrou, 2009). This is particularly the case in banks that have had difficulty with fraud in the past, as regulators in developed countries may discourage or even outright refuse their entry. However, regulators in developing countries may not be as rigorous and looser regulation in these countries may allow these banks to maintain fraudulent banking practices (Petrou, 2009) due to absence of stringent regulation. Ordinarily, conducting business in a consistent way would be a matter of business ethics (Weiss, 2008). However, for a company that is already business ethics would not matter. Benefits of international banks entering the Kenyan market include technological spill over and capacity increasing, improving financial mediation efficiency, improving credit access, and increasing financial stability as well as providing support for development activities (Claessens and Jansen, 2000; Clarke et al., 2002; Clarke et al., 2003).

2.5.2 Differences in Corporate Governance

A number of country characteristics play a role in determining what appropriate corporate governance is and how it is accomplished within individual country settings, particularly in regard to external environmental conditions (Doidge et al., 2007).

Banking structures in developing countries are often driven by business orientations that are at odds with Western ideas of transparency and fair dealing. For example, the Chinese banking system, which is based on relationships, is often considered to be highly corrupt by Western analysts (Horrocks et al., 2008). Research based on the Standard & Poor's transparency index and the corporate governance survey by the Institutional Shareholder Services (ISS) group found that country characteristics, including economic development, financial development, and legal and regulatory structures, are more important than firm-level characteristics in corporate governance, and that companies attempting to develop foreign direct investment will promote corporate governance standards (Doidge et al., 2007). Differences based on national culture priorities, including acceptance of litigation, legal formalism, and cultural value dimensions, in addition to legal structure, provides an improved model for corporate governance (Licht et al., 2005). There are some firm-level attributes that identify how a firm will implement corporate governance, including finance sources (government or private), board size, ownership concentration, and free cash flow (Chhaochharia & Laeven, 2009).

This implies that banks in Kenya will not only be affected by individual bank attributes but also by country characteristics such as Kenya's socio-economic, political, historic, legal and regulatory structures as well as corporate governance structures. These relationships are captured in the conceptual framework (Figure 3.2) and discussed largely in Chapter 3.

2.5.3 Consequences of Bank Fraud

Consequences of bank fraud can potentially involve bank failures and banking crises destabilizing the national economy. There has been little organised research into these

consequences in the Kenyan context. Thus, understanding what effects this has had in other contexts will help to demonstrate how the issues can be defined within this context and how they can be identified, as well as understanding the possible consequences for the Kenyan banking system and economy if fraud continues to go unchecked.

Extreme cases of bank fraud have the potential to highly disturb the economic system of a country. For example, in 1983, the Tel Aviv Stock Exchange (TASE) closed for 18 days following earnings management frauds attempts by the six main banks during a period of unusually high sell-offs (Blass & Grossman, 1996). The Turkish banking crisis of 2000 was also found to have likely been caused by systemic banking fraud, including the use of back to back loans intended to circumvent lending and capital requirements regulations (Soral et al., 2006).

One study that examined the relative losses on assets attributable to a bank's failure indicated that losses on assets could be as much as 30% of the failed bank's assets, with a further direct cost of closure of as much as 10% of the bank's assets (James, 1991). More recent analysis has shown that in addition to the direct cost of bank failure on the individual level, patterns of bank failure as have occurred in the United States, Spain, Japan, Norway, Sweden and Switzerland have cost taxpayers as much as three per cent of GDP in order to cover excess costs (Westernhagen, et al., 2004). Even if bank fraud is not levied directly against banks and customers within the host country, it can still prove to be detrimental to the country. Research has shown that the Nigerian Advance fee (419) banking frauds, although not generally levied against African banking customers, have had a negative effect on the perception of Nigeria and Africa as a whole (Vincent et al., 2004).

2.6 Responses to Fraud

Social and internal responses to fraud are important because they help to define the relationship between the banks and the fraud perpetrators and the general treatment of fraud in society, which will help to determine the overall cultural acceptance of fraud.

They also potentially serve as deterrents to committing fraud, making them important for consideration of the various factors involved.

2.6.1 Regulation and Harmonisation

One common external response to banking that may take place on a national or international level is that of regulation and harmonisation of banking rules intended to address the problem of banking fraud. This section examines the regulation and harmonisation efforts currently in place and examines their effects briefly.

There are three very common areas of banking regulatory requirements that may affect cost and profit efficiency as well as providing both areas for fraud and areas for fraud detection. These areas, derived from the Basel II accords, include capital adequacy (reserve) requirements, supervisory power, and market discipline mechanisms (Pasiouros et al., 2009). Research across 615 commercial banks in 74 countries across the 2000 to 2004 period showed that supervisory power by a central authority as well as market discipline regulations (including public disclosure of financial information) increases cost and profit efficiency. However, restrictions on banking activities, such as not allowing participation in non-banking sectors, increased profit efficiency but reduced cost efficiency; conversely increased capital requirements increases cost efficiency but reduces profit efficiency (Pasiouros et al., 2009).

Changes in regulation and reporting requirements have brought about changes in the type of fraud commonly perpetrated in the banking industry (Green & Reinstein, 2004). Changes in regulation resulting in reduction of fraud have been observed at least as early as the 1970s (Jaffe, 1974). Green and Reinstein (2004) indicate that while the degree of fraud has declined, there are still about as many individual fraudulent incidents in the banking system, at least in the United States. Under previous regulations that did not require high disclosure, fraud was commonly focused on the creation of fictitious information in order to support specific objectives; under the current high-transparency and public disclosure regime, fraud more commonly involves withholding information (Green & Reinstein, 2004).

One obvious example of changes in regulation that have brought about changes in potential fraud levels in Kenya is the liberalization of the Nairobi Stock Exchange in a drive to increase foreign direct investment in Kenya, which resulted in increased demands for transparency and imposed higher standards for corporate governance (Barako, Hancock, & Izan, 2006). However, simple changes in law and regulation cannot be relied upon to completely reduce or eliminate fraud; instead, there needs to be changes in attitudes surrounding fraud and its incidence as well as the regulatory changes in order to be effective (McBarnet, 2003). Until these attitudes change, McBarnet (2003) argues, the regulation is unlikely to be effective in challenging existing fraud rates.

There is evidence that banking industry harmonisation has significant benefits not only for the industry, but also for the growth of the economy as a whole (Romero-Avila, 2007). Romero-Avila (2007) found that increasing efficiency of financial intermediation drove economic growth in the European Union (EU) through the period of 1960 to 2001. This harmonisation, which included standardization of regulatory and process requirements for banks, increased the consistency of banking treatment (Romero-Avila, 2007). Banking industry harmonisation is one way in which developing countries could expect to benefit from regulation, as well as reduction of fraud. One example of this type of harmonization is the Basel banking standards, which are meant to impose a consistent method of banking regulation for issues such as reserves and deposit handling across different nations and regions (Benston, 1994). Compliance with this regulation helps the banks in their fight against fraud as the regulations provide for best practice, which if adhered to gives guidance on moral, ethical and other anti-fraud related issues. At the same time compliance means that Kenyan banking agencies have a higher rate of access to external sources of funds and other areas, which is a significant economic benefit (Benston, 1994). In particular, harmonized and consistent banking regulations make it easier for firms to access capital, thus allowing for a higher rate of growth across national borders rather than constraining the firm's market to a single country (Utrero-González, 2007). This provides a significant benefit for the firms and the economy as a whole.

2.6.1.1 Supervision

Bank fraud commonly emerges as a response to inadequate supervisory conditions (Evanoff & Kaufmann, 2005). Supervision at the government level is arranged in different ways depending on the jurisdiction. While the European Union has a central and single bank supervisory structure, the United States has shared bank supervision structures. This can lead to uncertainty regarding bank management, including the understanding of what would occur if the bank failed as well as who bears responsibility for losses from fraud. This can be particularly difficult in the case of international banks, where different levels of supervision and different supervisors may be present in the different countries. Thus, a bank that may be appropriately controlled in the home country may not be subject to appropriate oversight in other countries (Evanoff & Kaufmann, 2005).

2.6.1.2 Restriction of Business

Although banks may not detect initial fraud, they will have much stronger reactions following disclosed fraud by customers (Graham, Li, & Qiu, 2008). Specifically, companies that are forced to restate their earnings face higher spreads and interest rates and more demand for securing of loans than those that do not, as well as higher fees; those that have restated due to fraud are even further penalized. Thus, the bank can use contract terms to protect themselves from information asymmetries identified through these restatements (Graham, Li, & Qiu, 2008). However, it is uncertain how often this happens in Africa.

2.6.2 Human Resources Strategies (Recruitment and Selection)

One major individual response that banks may use in order to reduce fraud is to use recruitment and selection strategies to limit the exposure to those believed to be untrustworthy. However, this has not been very effective in the African context for a variety of reasons.

Human resources management practices, including recruitment and selection, are seen as a means of controlling for risk management (Meyer et al., 2011). However, some firms

in Africa (as in Meyer et al's study in South Africa) often have poor recruitment practices, such as not checking CVs or references prior to the hiring of the employee. Recruitment and selection practices including not checking CVs or references can often be seen to be related to structural issues, such as not being able to rely on support from previous employers and sabotage by employees (Meyer, Roodt, & Robbins, 2011). Thus, while firms should rely on recruitment and selection practices to lessen the potential for internal theft or other risks, in practice this may not always occur (Meyer, Roodt, & Robbins, 2011). Another issue, observed in Tanzania, is that a bank may outsource or share its back office operations, and in the process lose full control of the recruitment processes used to select the employees working on its accounts (Newenham-Kawindi, 2011). Furthermore, as in the Tanzanian case, the issue of social relationships and its impact on the recruitment practices may also influence the effectiveness of recruitment for risk maangement (Newenham-Kawindi, 2011). While it might be presumed that the risk of recruitment would be higher for positions such as clerks or cashiers, in fact this is not true; a study of Nigerian banks revealed that between 2000 and 2007, the most frequent perpetrators of fraud were supervisors, managers, or assistants in these roles (Owojori, Akintoye, & Adidu, 2011). As such, increased skills and responsibility cannot be substituted for effective recruitment practices.

There are a number of strategies that can be identified that are already in use in African firms to improve their recruitment and selection approaches in order to improve both human capital development and decrease risk. One potential strategy is the use of technical assistance from abroad, usually procured in the form of technical specialists. Technical assistance involves recruitment of Western specialists in the required area in order to provide support, training, and development services for the firm (Oshikoya, 2010). For example, banks could use technical assistance and Western recruitment in order to provide information technology skills to implement IT systems. Another approach that is increasingly used by African firms is internal development of human resources, including training of human resources specialists in order to better improve recruitment and selection practices. This system relies on improvement of the internal resources of the firm in order to improve the recuitment practices (Kamoche, 2011).

2.7 The Banking Environment in Africa

The previous section has discussed fraud from a global perspective. This section examines the banking environment in Africa focusing especially on existing evidence of corporate governance, fraud, and practises that differ from those of banks in Western countries. It provides specific evidence regarding the external conditions, including cultural, regulatory, and enforcement conditions that will affect the outcomes of anti-fraud measures in African banks.

2.7.1 Fraud in African Banking

Africa is commonly believed to have a higher rate of corruption than other regions of the world (Mbaku, 2007). The reasons given for this corruption are varied, ranging from institutional explanations such as relative weakness of postcolonial institutions or the lack of rule of law based on the failure of states to individual explanations such as strong collectivist or 'tribal' ties and the dominance of interpersonal relationships rather than contractual relationships (Mbaku, 2007). A cultural anomie explanation can also be posed, wherein corruption is significant due to the perception of economic disparities and economic hardships (Smith, 2008). This is particularly problematic given the issues with development aid and the formation of specific norms surrounding its use that encourage or even require corruption (Moyo & Ferguson, 2010).

Regardless of the reason for the high rate of corruption, it is clearly indicated on objective comparative measures that demonstrate that African countries are, in general, unusually prone to corruption. These metrics are tracked by Transparency International's Corruption Perception Index, which measures public sector corruption based on 13 separate surveys (Transparency International, 2010). Table 2.1 highlights the top and bottom ten CPI scores for countries in Africa, derived from Transparency International's Web site. Of these, Botswana was the highest ranking (least corrupt) of all 178 countries at 33, while Somalia was the last ranked country at 178 (Transparency International, 2010). In the 2010 index, Kenya has dropped among the ten bottom African nations at number 154 with a ranking of just 2.1, showing the problems that Kenya is likely to face

in managing fraud and corruption. Africa's general position at the bottom of this ranking indicates that it has a worse performance, at least on Transparency International's corruption model, than most other regions (See Appendix IIA and IIB)

Table 2.1 Top ten and bottom ten African countries as ranked by Transparency International CPI

Top Ten Countries			*Bottom Ten Countries*		
Country	Rank	CPI 2009 Score	Country	Rank	CPI 2009 Score
Botswana	33	5.8	Congo Brazzaville	154	2.1
Mauritius	39	5.4	Guinea Bissau	154	2.1
Cape Verde	45	5.1	Kenya	154	2.1
Seychelles	49	4.8	Guinea	164	2.0
South Africa	54	4.5	Democratic Republic of Congo	164	2.0
Namibia	56	4.4	Angola	168	1.9
Tunisia	59	4.3	Equatorial Guinea	168	1.8
Ghana	62	4.1	Burundi	170	1.8
Rwanda	66	4.0	Chad	171	1.7
Lesotho	78	3.5	Sudan	172	1.6
			Somalia	178	1.1

(Source: Transparency International, 2010)

General studies from African banking illustrate issues of concern to Kenya. A study of banking governance in Ghana found that there were considerable problems with corporate governance and fraud (Evans & Dadzie, 1998). This research, from the records of the Central Bank of Ghana during the 1990s showed that informed lenders charged higher fees for their loans (indicating potential bribes or other corrupt activity), and that prior relationships between lending officers and borrowers reduced enforcement of loan terms. This research does not provide a clear indication of corruption, although this was presented as one of the possibilities; it also suggested that lack of information or informal collection practices were evidence, as well as corruption in the general institutional structure.

In terms of fraud detection and prevention in African banking, evidence is scarce. However, one study showed that Nigerian commercial banks used relatively few risk management practices when engaged in information systems outsourcing (a potential source of external fraud). This study indicated that strategic, management, and information systems approaches were used only lightly in these banks, indicating a

serious lack in comparison to international banks, along with little regulatory attention to information technology (Adeleye et al., 2004). This both decreases competitive ability and increases fraud. Fraud innovations such as the Nigerian or 419 fraud, which commonly involves fraudsters using email to contact strangers, claiming to be sons or daughters of African diplomats, businessmen or other notables and extracting money due to implausible claims of large amounts of money, has made it clear that many African countries do not have sufficient fraud controls in place (Ampratwum, 2009).

2.7.2 Structural Adjustment

In many cases, the use of increased regulation in order to prevent bank fraud is actually restricted or discouraged in developing countries by financial policies that make external aid contingent on deregulation and liberalization (Grundberg, 1998). These changes are commonly made through programs such as World Bank structural adjustment programs, which require specific changes to the banking and economic system in order to drive foreign investment (Neu et al., 2008). These regulations are intended to benefit foreign direct investment (FDI) inflows by improving the economic environment and attractiveness of the host country; however, they also reduce the host country's ability to effectively oversee business and prevent fraud (Grundberg, 1998). Thus, rather than decreasing corruption and fraud in incoming industries, the use of financial liberalization regimes may actually increase it. This is a problem that has not yet been overcome by banking regulators in many countries. Although this problem is not unique to Africa, as Asian and South American countries have also undergone structural adjustment, it does play a significant role in development of conditions within these countries (and so needs to be considered).

Nigeria's experience with structural adjustment demonstrates how well or how poorly these regulatory demands may work. The IMF structural adjustment program in Nigeria, which began in 1986 under considerable economic pressure, called for a number of changes to be made to the regulatory environment in addition to other changes intended to reduce Nigeria's foreign debt load. These changes were intended to promote improved

investment climate, reduction of the deficit, and improvement of foreign exchange rates (Neu et al., 2008). This required reduction in regulation, public expenditures, and reorientation toward an export-led economy. It also came with considerable surveillance and oversight regulations by the IMF in order to ensure that the country was fulfilling its requirements (Neu et al., 2008). It was not only Nigeria that undertook this adjustment; instead, a large number of African countries, including Ethiopia, Kenya, Malawi, Tanzania, and Zimbabwe among others have undertaken a similar process of adjustment. The banking sector underwent liberalization and deregulation in keeping with these policies as well as the foundation of a deposit insurance program (Neu et al., 2008). Accounting technologies and other practices were also introduced. However, the reduction in regulation also left the banking industry without clear guidance in terms of accounting and reporting. This opened the door to considerable fraud and falsification of information throughout this period (Neu et al., 2008). Thus, the regulations intended to improve the efficiency of the banking system may have actually reduced its efficiency by increasing the opportunity for fraud.

Beginning in the mid-1990s, African governments began to reverse the structural changes required by the IMF as it became clear they were no longer effective (Kane & Rice, 2001). For example, in 1999 the Bank of Uganda increased its capital reserve requirements, and through the mid-1990s several African governments began to increase the amount of regulation banks were subject to. However, this was still insufficient to mitigate the damage to governments and depositors done by the lax regulation that allowed fraud to flourish. It also was insufficient to overcome a general atmosphere of corruption in some cases (Kane & Rice, 2001).

2.7.3 Bank Privatization and Regulation

One issue in African banking is the on-going or relatively recent privatization of banks. A study of banks in Nigeria from 1990 to 2001 demonstrated that a large number of banks had undergone privatization during this time (Beck et al., 2005). Furthermore, during this period there was also a development of significant difference in performance between privatized banks and those that remained under state control. Beck et al (2005) found that

privatized banks became more efficient and less fraud-driven than those that remained under state control. However, this research did not examine changes in regulation during this time that may have affected the outcomes of the research. The research also showed that banks that did not focus on lending, but instead on investment and bond management, have better performance than lending-based banks (Beck et al., 2005). It is possible that the issue of loan officer reluctance and conflicts of interest may have played into this, but that is uncertain.

2.7.4 Islamic Finance and Microfinance – Special Structures

Two areas where African banking systems differ from Western systems is in the use of Islamic finance and microfinance. These structures are not directly dealt with in this research, which focuses on the traditional Western-style commercial banking system. However, a brief word regarding them is appropriate in this case.

Islamic finance, intended to meet the needs of customers observing Islamic law particularly in regard to the payment or charging of interest, is becoming increasingly common throughout the Middle East and Africa, and is beginning to play a wider role in provision of financial services for Islamic observant individuals in these regions (Pryor, 2007). The first fully licensed Shariah compliant Kenyan banks are the Gulf African Bank (2007) and the First Community Bank (2008) (Wanyoike, 2011). However, there is little evidence regarding fraud in this case, and due to the relatively short establishment of these banks they were not included in this study.

Microfinance is an area of banking that does not commonly exist in the Western banking practice, but is very common throughout the developing world, especially in Africa. Microfinance is the practice of making very small loans (in many cases under $100 USD) intended to develop entrepreneurial activity in a given area (Krugman & Wells, 2006). Microfinance lenders, isolated from the formal banking sector and with limited access to fraud detection and prevention abilities and lower regulation rates, may suffer a higher rate of fraud, but actually use stronger social norms to prevent fraud (Arun, 2005).

2.8 Hypotheses

A number of hypotheses can be formulated following analysis of the literature. These hypotheses were posed in relation to three of the four following research questions:

1. What are the characteristics of fraud in the Kenyan banking industry?
2. What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?
3. How do banks approach fraud management?
4. Are there differences between the approaches to fraud management adopted by Kenyan and international banks?

2.8.1 Hypothesis 1

The first hypothesis is based on the size and geographic scope of the bank as compared to the size of the loss experienced within the bank. This hypothesis is related to the research question on the characteristics of fraud in the Kenyan banking industry. Murphy (1993) found that there was a linear relationship between the size of an organisation and the amount of fraud and theft, but a negative relationship between size and degree of supervision. Decreased supervision can lead to increase in fraud (Murphy, 1993).

The literature review identified that accounting transactions are affected by organizational characteristics such as the type of industry, organisational size, strategy and culture (Singleton and Singleton, 2010). This would suggest that fraudulent accounting transactions are influenced by the same factors. Research also shows that large organisations are more susceptible to higher incidences of fraud than smaller organisations as larger organisations tend to have more complex organisational structures (Singleton and Singleton, 2010; Holmes et al., 2000). This indicates that larger banks including those in Kenya could experience higher rates of fraud as well as offer greater opportunities and gains for fraudsters.

Holmes et al (2000) also found that not only the size of the organisation mattered in determining the amount of fraud but also the type of organisation, as larger government firms were more likely to become victims of fraud than smaller private firms. Barnes and

Webb (2007) found that larger organisations were found to be more susceptible to fraud than smaller organisations while public limited and private companies were found to be more susceptible to fraud and theft than public sector organisations, but that industry or sector did not affect fraud. This may suggest that the size of an individual bank in Kenya could determine its' susceptibility to fraud.

The discussion above leads to three initial hypotheses that will be used to examine the relationship between the size of bank and the amount (size) of the loss suffered by the organisation due to fraud. These hypotheses are similar in terms of their independent variable (size of the bank), but vary in terms of their dependent variable (including total loss to fraud, loss to fraud as a percentage of annual earnings, and loss to fraud based on a single event).

Hypothesis 1a: The total size of the loss to fraud will vary directly in proportion to the type or scope of the bank (where type or scope relates to whether the bank is international, national, regional or local)
Hypothesis 1b: The loss to fraud as a percentage of annual earnings will vary depending on the size of the bank.

2.8.2 Hypothesis 2

This second hypothesis is related to the research question on whether there are differences between the approaches to fraud management adopted by Kenyan and International banks.

Certain views have been expressed about the likelihood of prosecution. Abiola (2009) while researching into the relationship between poor salaries and fraud, and the relationship between fraud detection systems and fraud, in Nigeria hinted on the likelihood of prosecution, suggesting that Nigerian banks are likely to avoid prosecution if possible in order to avoid embarrassment or the market perception that they have been cheated or are vulnerable to being cheated. However, the disclosure and prosecution of fraudsters in international banks may be more likely, due to the practice of international

banks using bounties or bonuses for discovery and prosecution of fraud (Fisher et al., 2001). This could also be the case in Kenya.

There is also research supporting individual assumptions regarding the differences between international and regional or local banks. In a study of international firms in the Netherlands, it was found that international firms were high targets of crime and fraud, and that this led to a higher rate of prosecution among firms (Van Dijk & Terlouw, 1996). International firms are also likely to be interested in observing the laws and institutional rules of the country they are operating in, while domestic firms may have more social capital, reducing this need (Barker & Cobb, 1999). In many cases, international companies may be eager to prosecute fraud in order to avoid the appearance of corruption, which could provoke legal difficulties in their home countries or in other countries they operate in, such as in the United States under the Foreign Corrupt Practices Act (Lee & Hong, 2010). Findings of research conducted in the Middle East comprising respondents from different cultures indicated that what is considered to be fraud or corruption in one culture may not be transgressing cultural norms in another. This lack of common understanding of what constitutes fraud and corruption makes it difficult to fight and prosecute fraud locally and internationally (Watson, 2003).

Based on the above discussion, hypothesis 2 is proposed as follows:
Hypothesis 2a: Banks that are international banks or international subsidiary banks will be more likely to use criminal prosecution or civil action against fraudsters than national, regional, or local banks.
Hypothesis 2b: Banks will be more likely to use criminal prosecution or civil action against external parties than against internal parties.

2.8.3 Hypothesis 3

Hypothesis 3 draws from the research question on how banks approach fraud management. There is considerable practical evidence for the use of internal security and auditing protocols, training, and other mechanisms for control of internal fraud, and their effectiveness within the organisation in terms of controlling fraud at the corporate culture

level (May, 2003; Singleton, Singleton, & Bologna, 2006). However, this research is not uniform. Research by Barnes and Webb (2007) indicates that there is no relationship between the size of fraud loss and the nature of management controls employed by the organisation. There may also be a cultural element to the effectiveness of management controls, as traditional management controls have proved to be more effective in a Sinhalese organisation than were imported, stricter control practices from privatised international owners (Wickramasinghe & Hopper, 2005). Furthermore, management controls have proved to be ineffective in cases such as Enron, where strong management controls were undermined by the development of a culture where management fraud was prevalent (Free & Macintosh, 2007). However, some types of controls, such as strong records management, are significantly associated with a reduction in fraud (Palmer, 2000). Given this conflicting information, it is likely that the use of procedural and management controls for fraud will reduce fraud, but possibly only in certain ways.

Size of the organisation is also a determining factor in how the firms will choose organisational security protocols. In a study of major Australian firms, larger firms were found to have more effective data management protocols (Nord, Nord, & Zu, 2005). Larger organisations have also been found to use internal auditing approaches more commonly than smaller organisations (Coram, Ferguson, & Moroney, 2008). Furthermore, smaller organisations are associated with more reluctance to identify fraud even in cases where it is clear given the existing security protocols (Keenan, 2000).

Given this evidence, Hypothesis 3 is posed:

Hypothesis 3a: The use of procedural and auditing approaches to fraud detection and monitoring will result in lower occurrence of fraud.

Hypothesis 3b: Large organisations will be more likely to adopt organisational security protocols than small organisations.

2.9 Summary

This chapter has presented the most relevant secondary information identified by the researcher in the literature for the area of research. The fraud theories provide an understanding about the nature, characteristics and behaviour of fraud and those who perpetrate fraud. A theoretical and contextual framework has been laid by identifying the economic foundations of fraud, corporate governance practices, types of banking fraud and aspects of fraud detection and prevention. The body of empirical evidence for fraud in the banking industry has been examined, presenting specific information and evidence regarding areas such as the use of software and auditing practices for the areas of concern. The chapter further explored why international banks set up a presence in developing countries. The importance and challenges of bank governance, regulation and harmonization, deregulation, supervision and law enforcement have been considered. This chapter also provided contextual evidence for banking in Africa, including special concerns of African banking as well as evidence regarding the management of bank fraud in Africa. From the literature presented above it is clear that most of the research and studies on fraud and fraud prevention have been carried out in very few countries, notably, the United States of America, Great Britain and Australia. This justifies and presents a strong case for more fraud research in Africa.

Chapter 3
Contextualising Kenya's Banking Industry

3.1 Introduction

This chapter introduces Kenya's banking system highlighting the historical, economic and social-political issues that have affected the banking industry. The chapter sets the background and context in which the banking industry operates and serves to enhance the understanding of the development of this industry. Discussion in this chapter includes the structure of the banking industry (Section 3.1) and historical, political, economic, legal, technological, regulatory and other factors that influence the banking industry (Section 3.2 – Section 3.9). Section 3.10 presents the construction of a conceptual framework intended to support the findings. This information discusses primarily the external factors involved in the development of fraud within the banking industry.

3.2 Structure of the Banking industry

The Kenyan banking system falls under the auspices of the Central Bank of Kenya (CBK). The CBK is an independent Central Bank that engages with fiscal and monetary policies for the Kenyan government as well as oversight of the Kenyan banking industry (Central Bank of Kenya, 2007; Central Bank of Kenya, 2008c). Other than formulating or implementing monetary policies the CBK fosters the liquidity, solvency and proper functioning of the banking and financial systems in Kenya (Central Bank of Kenya, 2007). As at the end of December 2010 the banking sector comprised of 43 commercial banks, 1 mortgage finance company, 5 deposit taking microfinance institutions (DTM), 2 representative offices of foreign banks and 126 foreign exchange bureaus which are all private and mostly locally owned (Bank Supervision Report, 2010). This included 33 locally owned institutions and 12 foreign owned institutions (Bank Supervision Report, 2008). The local banks included three state-owned or primarily state-owned institutions, 28 privately owned institutions and 2 mortgage finance institutions. The foreign owned banks consisted of 8 locally incorporated foreign banks and 4 branches of foreign incorporated banks. Figure 3.1 demonstrates this arrangement and structure of the

Kenyan banking industry. Additional components of the financial sector in Kenya that will not be studied include micro finance institutions, insurance companies and the Nairobi stock exchange. Further information regarding the banking sector in Kenya is found in Appendices IIC and Appendix IID

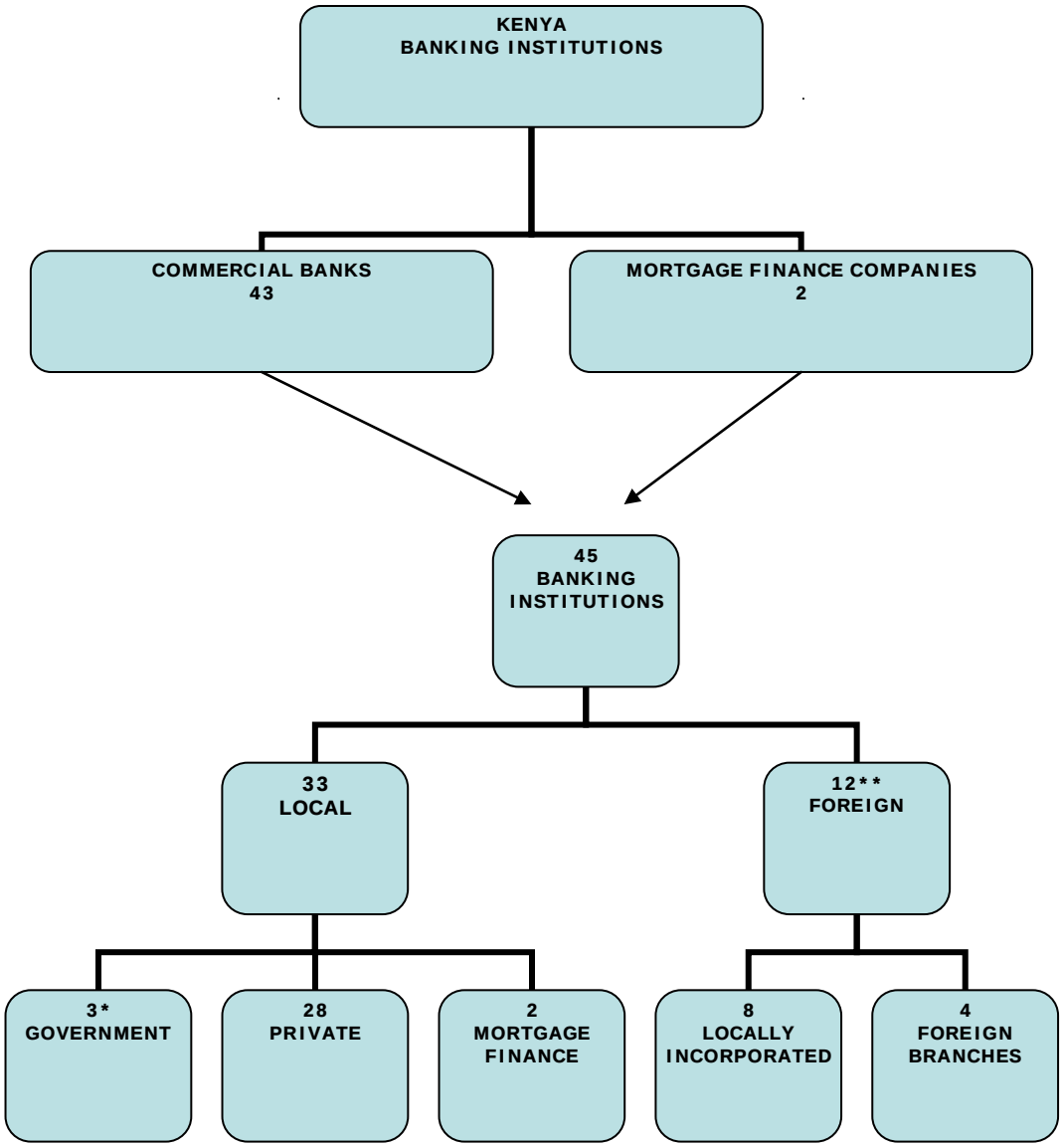


Figure 3.1 Ownership structures of commercial banks and mortgage finance institutions in Kenya (Source: Bank Supervision Report, 2008; Central Bank of Kenya, 2008b)

Table 3.1 summarizes the number of banks, mortgage finance companies (MFC), micro finance institutes (MFI), representative (REP) offices, deposit taking micro finance

institute (DTM), building (BLDG) societies and foreign exchange (forex) bureaus between 2006 and 2010.

Table 3.1 various types of banks in Kenya

Year	No. of Banks	Commercial Banks	Mortgage Finance Companies	Micro Finance Agencies	Rep Office	Building Societies	Forex Bureaus
2010	44	43	1	-	2	5	126
2009	46	44	2	-	-	-	130
2008	45	43	2	-	-	-	120
2007	45	42	2	1	-	-	97
2006	45	41	2	1	-	1	95

(Source: Bank Supervision Reports, 2006-2010)

Large banks (comprising 14 banks) dominate the market and hold over 80% of the total net assets, net advances, customer deposits and capital reserves. The remaining 20% of the net assets are shared among medium size banks (13%), small banks (4%) and other financial institutions. The big banks tend to enjoy high profitability, 90% of the total profits in the banking sector, while several other banks are affected by non-performing loans (Bank Supervision Report, 2008).

3.3 History and growth of the banking industry in Kenya

This section outlines the dynamic nature of Kenya's banking industry and lays out various factors that have contributed to strengths and weaknesses in the industry. Some of these factors have encouraged mismanagement and fraudulent practices within the industry.

3.3.1 History of the Banking industry

Kenya has a long history of commercial banking that goes back to 1896 when the National Bank of India opened a branch in Mombasa, Kenya. Kenya's financial system grew faster post-independence than most other sub-Saharan African countries (Brownridge, 1998). By the time of independence in 1963, Kenya had 10 commercial banks. 80% of the market share for bank deposits was held between three big banks - National and Grindlays Bank, Barclays Bank, and Standard Bank (Kenya Commercial Bank, 2011). On achieving independence there was a need to develop a more locally oriented banking system. Thus, upon independence the Government of Kenya (GOK) substantially nationalized the National and Grindlays Bank by acquiring 60% of its shareholding. The GOK was later to acquire 100% of the National and Grindlays shares in 1970, taking full control of Kenya's largest commercial bank and subsequently renaming it the Kenya Commercial Bank (KCB). Today KCB boasts the largest branch network in Kenya (Kenya Commercial Bank, 2011). Other than the KCB two more banks were established in 1970: the Cooperative Bank of Kenya and the National Bank of Kenya (NBK). By the early 1970s the Kenya Commercial Bank and the National Bank of Kenya held between them 35% of the paid up capital while the Barc1ays Bank and the Standard Bank accounted for about 22% each. In view of the move towards divesture, the two governments owned commercial banks (KCB and NBK) sold 40% of their shares to the public between 1988 and 1996 (Ngugi & Kabubo, 1998)

The global economic recession of the mid-2000's had little direct effect on the Kenyan economy. The Kenyan Banking Sector remained strong in the wake of the global financial crisis due to low levels of their participation in or weak financial linkages to global financial markets (Bank Supervision Report, Annual report 2008).

Commendable progress has been made in improving access to financial services in Kenya over the past few years. This increase in accessing financial services is attributed to the increased use of non-bank financial institutions, especially companies that are providing mobile phone money transfer services such as Safaricom (MPESA) and Zain (SOKOTELE) that more than doubled demand for financial services from 7.5% in 2006

to 17.9% in 2009. By the end of December 2009, MPESA had attracted over 9 million registered customers and 16,000 agents country-wide (Bank Supervision Report, 2009).

3.3.2 Changes in the banking industry

Despite the rapid development witnessed in the financial system, Kenya's capital market still remains relatively young. With a banking industry that stands at just over 40 commercial banks and several foreign exchange bureaus, Kenya's banking industry is relatively large. In the past 2 decades the banking industry has undergone changes due to mergers, acquisitions and conversions.

As a result of changes in the operating environment a number of commercial banks and other licensed institutions have opted for mergers and acquisitions. Between 1994 and June 2010 there have been 32 successful mergers. The details of specific banks that merged are shown in Appendix IIE. Only three acquisitions have taken place to date (as shown in Appendix IIE). Over the years several non-bank financial institutions (NBFIs) have transformed or converted themselves into commercial banks by meeting the minimum prudential requirements for commercial banks as far as capital adequacy, liquidity and assets requirements are concerned. Details of the specific bank conversions as well as a comparative graph showing mergers, acquisitions and conversions are contained in Appendix IIF.

In the face of the second wave of banking failures in 1993-1994, the Central Bank of Kenya tightened the Banking laws in 1995 requiring all Non-Bank Financial Institutions (NBFI) to convert to Commercial banks or face closure.

3.4 Legal, Regulatory and Policy Frameworks of Banking

The Companies Act (Chapter 486, Laws of Kenya) the Banking Act (Chapter 488, Laws of Kenya, 2009) and the Central Bank of Kenya Act (Chapter 491, Laws of Kenya) provide the main legal framework for banking in Kenya, in addition to best practices. The Central Bank is legally empowered through the Central Bank Act and Chapter 492 of the

laws of Kenya to oversee the performance of the financial and banking systems in terms of solvency, liquidity and stability of the financial systems. The Central Bank also regulates and supervises the money market while enforcing the Banking Act and prudential guidelines for best practices in the industry. The Bank also works closely with the Institute of Certified Public Accountants of Kenya (ICPAK) to ensure that the banking sector leads the other sectors in the implementation of International Accounting Standards (Centre for Corporate Governance, 2004). Other regulating and legal bodies include the Kenya Bankers Association (KBA) and the Capital Markets Authority (CMA).

The capital market is part of the financial system that provides funds for long-term development and brings together lenders (investors) of capital and borrowers (companies that sell securities to the public) of capital (Capital Markets Authority, 2011). The CMA's main goal is to provide long-term credit, reducing pressure on the government and expanding capital market ownership.

The Kenya Bankers Association is a self-regulating body dealing with bank operational rules and procedures. On the 16th July 1962 the Kenya Bankers (Employers) Association was registered as a Trade Union to cater for the employment rights of bank workers. In April 1968 a separate sister body called the Kenya Bankers Association was registered under the Societies Act to take care of other social and business interests of bank workers. However, in the year 2000, the two Associations merged together to create the Kenya Bankers Association, embracing the functions of the two bodies. The Association's membership consists of the 43 Commercial Banks (African Banking & Finance Conference, 2010).

Policy reforms have seen a shift in the banking sector from total control by foreign investors at the time of independence to one that now has significant local ownership (Ikiara, Nyandemo and Ikiara, 2003). Government divesture has also played a role. Over the past two decades (since around 1990) the government has sold most of its shares in banks like Kenya Commercial Bank, National Bank of Kenya and Housing Finance

Company to the public and private sector. Policy in the banking sector has remained relatively liberal since the 1980's with restrictions on paid up capital for foreign banks and foreign shareholding of listed banks being relaxed. After the implementation of the World Bank sponsored Structural Adjustment programmes (SAPs) a number of reforms were initiated in the financial sector with an aim of tightening the regulatory environment, fostering competition and enhancing efficiency (Ikiara, Nyandemo and Ikiara, 2003).

The legislative framework for the banking industry was provided by the Banking Act of 1968, which replaced the banking ordinance enacted under the colonial era. This legal framework and CBK's supervisory responsibilities evolved to regulate a banking system confined to subsidiaries of multinational or international banks that had strong internal controls and qualified staff. Conversely, with the advent of local financial institutions in the 1970's the demands placed on the bank supervisors changed. Financial institutions begun to mushroom but they were often fraudulently and incompetently managed and lacked the required capitalization (Brownridge, 1998). This can be blamed on the relaxed regulatory and supervisory systems prevalent and operating in the banking and financial systems at this time, which cultivated a culture of poor governance and weak management in the industry. Clear laws, rules and regulations need to be set up to legislate and regulate the banking industry to enable effective legal enforcement (Gikandi and Bloor, 2010).

3.5 Kenya's Banking Crises: 1980-1990

Kenya has experienced two major waves of banking crises that have affected the industry and encouraged fraudulent practices within the industry. These crises provide an understanding of history that has influenced management in the banking industry.

Immediately after independence in 1963 the Kenyan banking and financial system can be described as one that was highly controlled by the government. In 1982 the government relaxed some of the strict rules that had been placed on the issuance of licenses. This encouraged a number of non-bank financial institutions (NBFIs) to join the banking

industry. The government also introduced a low capital requirement of KES 5 million that could easily be raised (Centre for Corporate Governance, 2004). By the onset of financial reforms in the mid-1980s, the number of licensed commercial banks had doubled to 24, comprising of 15 foreign-owned, 3 state banks and 6 locally-owned private banks (Mwega, n.d.). The mushrooming of financial institutions in the 1970's coupled with lax banking laws, inadequate CBK supervisory capacity and the use of political connections by some banks to override the banking laws resulted in deficiencies of the banking system that ushered in several bank failures (37 bank failures as at 1998) in the 1980s and 1990s.

A total of 10 NBFIs and 2 banks were closed or taken over in the period 1984-1989 and a further 10 NBFIs and 5 banks in 1993-1994 (Brownridge, 1998b). In spite of the efforts of the Central Bank and the Treasury to bail out the ailing institutions, the Rural Urban Credit Finance collapsed in December 1984, under a cloud regarding fraudulent political involvement that resulted in a high non-performing debt load (Brownridge, 1998).

An amendment to the Banking Act in 1985 expanded the safety net by putting restrictions on insider or connected lending, raising the level of minimum capital requirements (to KES 15 million for a bank and KES7.5 million for a NBFI) and tightening the licensing procedure. At this point in time several financial institutions had secured funds from parastatal organisations and suffered liquidity crises when the same parastatals suddenly withdrew their deposits supposedly for political motives. Some financial institutions flaunted lending procedures or attempted to squeeze interest rate margins. Poorly qualified managers were also often appointed from among less able employees (Brownridge, 1998; Central Bank of Kenya, 2008). Other than poor management practices, bad governance and weak internal controls were prevalent during this period. The Continental Bank of Kenya Limited and Continental Credit Finance Limited collapsed in 1986 and Capital Finance Limited followed in 1987. Seven collapsed banks were merged to create Consolidated Bank of Kenya Limited in 1989.

In response to the first wave of crisis (1984-6) the Deposit Protection Fund Board (DPFB) was established in 1986 as a deposit insurance scheme to provide cover for depositors and act as bank liquidator. The same amendments gave Central Bank of Kenya the responsibility of risk minimization through enhanced prudential regulation, supervision and surveillance. The function of curator and revival of ailing institutions was also entrusted to the Central Bank (Central Bank of Kenya, 2008).

Eleven institutions were placed under liquidation in 1993. Ten of these were under the DPFB while one went into voluntary liquidation. Further failures were seen, however, including two in 1994, three in 1996, one in 1997, five in 1998, one in 1999, one in 2001, two in 2003, and two in 2005 (Central Bank of Kenya, 2008).

Shared characteristics in bank failures in the 1980s and 1990s include strict ownership control (individual or family), concentrated lending decisions and policies, and mismanagement of loans including disbursement of loans without collateral, documentation, or credit-worthiness of borrowers (Brownridge, 1998). The majority of banks thus collapsed due to fraudulent or imprudent lending, which was often politically linked (Brownridge, 1998). This could have been avoided by independent management (Brownridge, 1998b). A further factor was a rush to privatization from government control, which compounded the problem by introducing a weak institutional environment and ineffective legal and regulatory controls as well as sale to connected individuals, reducing the overall benefit of privatization (Beck & Fuchs, 2004). Other causes of failure included inadequate capitalization, excessive insider lending resulting in non-performing loans and adverse selection of borrowers (Brownridge, 1998). In particular, insider loans to politicians and others for speculative ventures such as real estate resulted in a mismatching of bank asset and liability maturities (Waweru and Kalani, 2009). This is consistent with evidence from other banking environments showing that fraudulent or unsound banking practices by managers are implicated in failure of banks (Rezaee, 2001).

3.6 The Goldenberg Scandal

One of the largest scandals so far in Kenya's history is what has become popularly known as the Goldenberg Scandal. This scandal involved two companies, Goldenberg International Limited and the Exchange Bank Limited. These two companies were related as they shared common shareholders, promoters and directors[1] (Republic of Kenya, 2005). Goldenberg International was registered in 1990 as stated in its Articles of Association (Article 3(a) and (b)) to:

"3 (a) To carry on the business of import and export in any or all types of minerals, gold, silver, diamonds, precious and semiprecious stones … in Kenya to all PTA countries, Europe, India and other parts of the world.

(b) To prospect, explore, open and work claims or mines and raise dig and quarry for gold, silver, mineral ores … diamonds, precious and semi-precious stones … in Kenya and in other parts of East Africa."(Republic of Kenya, 2005, p.36)

There is no evidence that Goldenberg International ever engaged in the activity for which it was registered, and Kenya has few sources of gold or diamonds. It is therefore largely believed that Goldenberg International brought in gold and diamonds from the Democratic Republic of Congo and exported the same while maintaining that they processed the minerals from Kenya. There was also no evidence of the company having other shares allotted and paid for from anyone else except the two directors. The Exchange Bank was officially registered and licensed to operate by the Ministry of Finance in 1991 with a proposed capital of 40 million Kenya Shillings (KES). Like Goldenberg International Limited, there was no evidence that other persons had been invited to take up shares in Exchange Bank Limited. No register of members existed, no copies of share certificate were available and at no time had the Central Bank of Kenya confirmed that the Exchange Bank had the proposed nominal capital (Republic of Kenya, 2005). Although there are clear signs that this was a fraudulent company, economic and political upheaval in the Kenyan government allowed the firm to be established.

[1] Kamlesh Pattni, the 25 year old son of a gold jeweller dealer in Mombasa and Mr. Kanyuto, the then Director of Intelligence with the Kenya Police. He was also a Director in the First American Bank and Firestone East Africa

To sum it up the Goldenberg Affair was nothing "but a series of business deals or alleged business deals revolving round various economic schemes" that related to "Export Compensation, Pre-shipment Finance, Retention Accounts, Convertible Foreign Exchange bearer certificates (Forex C), Spot and Forward Contracts, cheque kiting and outright theft" (Republic of Kenya, 2005, p.35). The government had set up an export compensation scheme and through it paid out incentives to Goldenberg International for the supposed export of gold estimated at USD80 Million (BBC News, 2006).

Even though it is largely acknowledged to be fraud, this case has been difficult to prosecute as the scandal is largely believed to have involved prominent people and top government officials[2]. Economically, the Goldenberg Affair has cost the tax payer over USD600 million with another estimated USD1 Billion believed to have been siphoned out through the Goldenberg connections. At the time this scandal erupted in 1993 the losses from this fraud were estimated at an amount equal to 10% of Kenya's Gross Domestic Product (Republic of Kenya, 2005; Family News Forum, 2010; BBC News, 2006).

In 1993 when the scandal broke the Exchange Bank was closed down due to failure to honour foreign exchange contracts. Other banks that had dealings with Goldenberg International Limited went into liquidation at around the same time, including the Trade Bank, Post Bank Credit Ltd., Delphis Bank Ltd., Trust Bank Ltd. and Pan African Bank. This heralded the second wave of the banking crisis in Kenya.

There were a number of effects from the Goldenberg Scandal. The Parliamentary process of scrutinizing financial and legal documents had to be addressed and the Central bank had to review legal and regulatory mechanisms. The office of the Auditor General was also held to account for the removal of qualified staff and their replacement with less

[2] Those allegedly charged include former intelligence chief James Kanyotu, former treasury permanent secretary Wilfred Karuga Koinange, former Central Bank governor Eric Kotut and his deputy Eliphaz Riungu. Among those mentioned adversely in this case were, the former President's (Moi) two sons – Gideon and Philip, two former Vice Presidents, prominent business men and senior civil servants. The Goldenberg Commission report states that the former President, Moi, and the then Finance Minister, George Saitoti, have a case to answer as they must have been aware of the scam. The top executives of the Department of Mines and Geology are also included here.

qualified staff that were not competent enough to produce audited accounts for the Parliamentary Accounts Committee. The police did not move swift enough to arrest the perpetrators, nor did the Attorney General rise to the occasion by bringing a case against the perpetrators. Instead the Goldenberg scandal was first brought to court by the Law Society of Kenya, while the judiciary system actually impeded progress (Republic of Kenya, 2005). The Goldenberg Scandal continues to be implicated in Kenyan socioeconomic and monetary losses as well as affecting the financial services industry.

3.7 Moral Hazard and Adverse Selection in Kenyan Banks

Moral hazard arises when individuals, or a group of individuals, prioritizes their interest or/and possible financial gain without giving a thought to the moral implications of their decision. It involves a trade off between risk and return and is mainly characterized by asymmetric information (Brownridge, 1998b). Kenya's banking crisis of the early 1980's and 1990's was precipitated by the presence of moral hazard and adverse selection. Some banks were lending without regard to the stipulated minimum capital requirements set by the CBK. As argued by Brownridge (1998a), moral hazard is inversely related to bank capital. Poorly capitalized banks have not invested much of their own money and rely mainly on capital provided by other people. Such banks therefore do not stand to lose much by investing in risky ventures.

Brownridge (1998b) further argues that moral hazard becomes more severe when banks engage in insider lending. Insider lending is profitable when profits arise from the project as these profits will all be internal profits. However, when the projects return losses the bank will have to bear the full brunt of the loss, having no external party to share the loss with. As proved in the case of Kenya's banking crisis, insider lending is a leading cause of bank failures worldwide (Caprio, 1997, Pg.6-7, cited by Brownridge, 1998b).

Factors involved in moral hazard include information asymmetry (when one party is more informed than another and thus has a greater advantage in terms of negotiation power) (Stiglitz and Weiss, 1981) and adverse selection, or the process of sorting potential borrowers and "is a consequence of different borrowers having different

probabilities of repaying their loan" (Stiglitz and Weiss, 1981, Pg.393). An adverse selection problem arises when a borrower who borrows at a high interest rate is unable to repay the loan leading to reduced profits to the lender. Several "political banks" were affected by the effects of adverse selection during the era of the banking crisis, after loans to politicians at a high interest rate resulted in default and eventually liquidation of the banks. Non-performing loans still remain a problem in Kenya today. This is shown by on-going high interest rate spreads (high lending rates) and low deposit rates. With increasing competition for customers in the banking industry, adverse selection of borrowers and moral hazard will only get worse, leaving local banks more exposed to these hazards due to less credit-worthy borrowers (Brownridge, 1998b).

3.8 Developments in the Legal and Supervisory Framework

The CBK in collaboration with the Ministry of Finance champions legislative reforms for enhancing stability, safety, efficiency, accessibility and integrity within the banking system. In 2008 the Microfinance Act was made operational, the publication of the Credit Reference Bureau regulations took place, the Proceeds of Crime and Anti-Money Laundering Bill, 2008 was tabled in Parliament and Presidential Assent was given to the Finance Act, 2008.

3.8.1 Credit Reference Bureaus (CRB's)

Publication of the Banking (Credit Reference Bureau) Regulations, 2008 on 11th July 2008 and the operationalization of the same on 2nd February 2009 marked a milestone in Kenyan banking. These regulations empower the CBK to license and oversee Credit Reference Bureaus that will collate credit information from banking institutions on non-performing loans, dishonoured cheques (other than on technical reasons), proven cases of fraud, forgeries and cheque kiting, false statements and declarations, tendering false securities and misapplication of borrowed funds. The Central Bank of Kenya received three applications for CRB licenses before end of 2009 from the Credit Reference Bureau Africa Limited (CRB Africa), Metropol Credit Reference Bureau Limited (Metropol) and Compuscan (K) Limited (Compuscan). However, only CRB Africa has been approved as of August 2009 (Bank Supervision Report, 2008; Bank Supervision Report, 2009). As at

30th September 2010, banks had accessed 103,332 credit reports. The uptake of credit reports by banks' is expected to increase as use of credit referencing is entrenched in banks' credit appraisal processes (Bank Supervision Report, 2010).

3.8.2 Proceeds of Crime and Anti-Money Laundering Act

The AML Bill became an Act of Parliament in December 2009. The Act is significant as it represents the first step Kenya is taking in criminalizing the offence of money laundering. This Act establishes the Financial Reporting Centre, the Assets Recovery Agency and the Anti-Money Laundering Advisory Board. It allows for the confiscation of wealth and assets arising from money laundering by instituting procedures for both civil and criminal forfeiture. The AML Act establishes procedures for international assistance in investigations and proceedings enabling banks to work with other banks world-wide to fight the money laundering crime as well as reinforcing financial integrity (Bank Supervision Report, 2009; Bank Supervision Report, 2010).

3.8.3 The Finance Act

Every year the Finance Act is amended for changes and developments in the legal and supervisory arena. Importantly, the Finance Act of 2009 gave the Central Bank of Kenya permission to share bank information with fiscal or tax agencies and fraud investigation agencies.

3.8.4 IT Usage

There has been a marked increase in ICT investment by banks in the industry. ICT investment has been driven by customer awareness of and demand for ATMs and related services such as mobile phone and Internet banking, as well as improved efficiency (Bank Supervision Report, 2009; Bank Supervision Report 2010).There has been a noticeable improvement in staff – customer ratio from 1:60 in 1996 to 1:252 in 2008 (Bank Supervision Report, 2008).

As at December 2010, 33 out of the 44 bank institutions were providing electronic banking, while 19 banks offer overseas electronic money transfer services in

collaboration with various international money transfer agents. Other e-banking services introduced by financial institutions included the electronic viewing and retrieval of bank accounts and statements via email, balance enquiries, cheque book requests and enquiries on status of cheques, notification on purchases and withdrawals made by the customer, transfer of funds between designated accounts and utility payment services and mobile phone top ups.

The security of electronic banking in Kenya is questionable. Recent reports indicate that electronic funds transfer systems, created loopholes for fraud (Irungu, 2011) representing 69% of the total fraud reported in the second quarter for 2010 (Irungu, 2011). This suggests that e-banking is exposing banks and rendering them more vulnerable to fraud.

Developments in information technology have also stimulated competition from the mobile phone industry. Since the advent of the mobile phone money transfer services in March 2007 with Safaricom's M-Pesa service, other mobile operators have registered over 15 million customers (Bank Supervision Report, 2010). The M-Pesa service had facilitated the transfer of more than KESS23.77 billion by October 2008($339.5 million) (Anon, 2008). It is estimated that 13 million Kenyans own mobile phones, and that 73% use mobile banking services (Government of Kenya, 2008). M-Pesa remains the fore-runner in the mobile phone money transfer industry, shifting 305.7 million transactions valued at approximately US$8 billion (KShs727.8 billion). This has prompted banks to respond to customer needs by entering into partnership with mobile phone transfer service companies to provide mobile banking services to banking customers. Banking services offered by commercial banks include ZAP (Standard Chartered Bank in collaboration with mobile phone provider Zain) and EAZZY 24-7 (a partnership between Safaricom and Equity Bank), among others (Bank Supervision Report, 2010). There are already indications that cases of fraud are surfacing in the mobile phone transfer services. In 2010 fraudsters reportedly stole US$233,333 (KShs21 million) through Safaricom's M-Pesa money transfer system (Irungu, 2011).

3.8.5 Agent Banking

The agent banking model allows financial institutions to provide banking services in areas where there is no direct need for a physical branch, but there is a need for banking services, reducing the cost of service provision and expanding services for the unbanked. This new model eliminates the need for a physical bank building and reduces costs while providing convenient banking services for the public (Risk Management Survey, 2010). This model is being used in other developing countries like India and several South American countries such as Brazil, Peru, Colombia, Chile and Mexico. Brazil currently operates the largest agent banking system in the world.

Since the coming into operations of the Guidelines on Agent Banking in May 2010, six banks have applied to the CBK for Agent Network approval. Of these, two applications had been granted approval by end of September 2010, while the other four are at various stages of review. As at 30th September 2010, CBK had approved 5,892 agents of which 4,392 of these agents are linked to the telecommunication business with 1,500 comprising other types of enterprises. Two thirds of agents are in rural areas. The principal-agent problem poses a fraud risk and banks must carefully investigate agents before appointing them (Wafula, 2010). There are also issues in regulation and legal frameworks for this type of banking (Consultative Group to Assist the Poor, 2011).

3.9 Regional growth and networking

Kenyan banks have continued to spread into the East African regions. The East African Central Banks of Kenya, Uganda, Tanzania, Rwanda and Burundi finalised a Memorandum of Understanding (MOU) in late 2008 that is aimed at facilitating information sharing and supervisory co-operation especially for banking groups that are regional. With the banks leading the way, by the end of 2009, similar arrangements were achieved between the Insurance Regulatory Authority (IRA), Capital Markets Authority (CMA) and the Retirement Benefits Authority (RBA). These initiatives highlight the growing need for co-ordination first amongst the domestic regulators and then amongst foreign and domestic regulators. It is anticipated that banks will continue to explore new

regional opportunities and consolidate their market niches (Bank Supervision report, 2008; Bank Supervision report, 2009)

Through various initiatives led by World Bank, International Monetary Fund and the Financial Stability Institute (FSI) strategies are being laid to enhance the harmonization of supervisory practices. Meanwhile the CBK is currently involved in efforts to establish monetary unions by the East African Community (EAC), the Common Market for Eastern and Southern Africa (COMESA) and the African Union (AU). The EAC and COMESA are building blocks for the African Monetary Union. The plan is that through the Monetary Affairs Committee (MAC), an EAC Committee tasked with the mandate of laying the foundation for a common monetary union, one currency and one Central Bank will be established in East Africa. Such growth emphasizes the need for harmonisation of supervisory policies, practices and procedures.

Even though regionally Kenya's banking and financial systems are relatively well developed it has not achieved its full potential due to structural barriers and weaknesses (Beck and Fuchs, 2004). Expanding operations into new regions will further complicate these structural barriers due to the imminent challenge of cross-border fraud and risk management.

3.10 The Conceptual Framework

Following examination of the literature, theoretical and empirical research that has been conducted, a conceptual framework has been designed that takes into account a number of the requirements of the study and identifies potential areas of influence on the practice of fraud. The conceptual framework is shown in Figure 3.2. The conceptual diagram separates the internal and external industry factors. The internal factors represent bank specific and inter-bank factors while the external factors represent factors from without the banking industry that impact on fraud management.

The conceptual framework begins with the core of the fraud – the perpetrator, or individual committing the fraud, and his or her motivation. Thus, the first component of

the conceptual framework is represented by Cressey's fraud triangle formed by the three elements of pressure, opportunity, and rationalization (Cressey, 1973; Wells, 2005).

The second component is the internal industry factors, including factors that both encourage and discourage fraud, such as information sharing, inter-bank competition, organisational characteristics, insider involvement, internal controls, and information technology (Barth et al, 2008; Breuer, 2006; Canhoto & Backhouse, 2007; Cressey, 1973; Holtfreter, 2005; Macey & O'Hara, 2003; Smigel, 1956; Wells, 2004; Zahra, Priem & Rasheed, 2007).

The third component is the external industry factors. These include legal factors like regulation and law and enforcement as well as general governance environment (Aguilar, Gill & Pino, 2000; Barth et al., 2008; Doidge, Karolyi, & Stulz, 2007; Licht, Goldschmidt, & Schwartz, 2005; Macey & O'Hara, 2003; Wilhelm, 2004). Ethical factors also play a role (Aguilar, Gill & Pino, 2000; Cressey, 1973; Schmidt, 2005; Wells, 2005). Sociocultural factors such as corruption and acceptable business practices must also be considered (Bakre, 2007; Transparency International, 2009; Zahra, Priem & Rasheed, 2007). The use of information technology in society generally is also considered at this level (Fernandez & Gonzales, 2005). Further factors considered include political, economic, and customer factors.

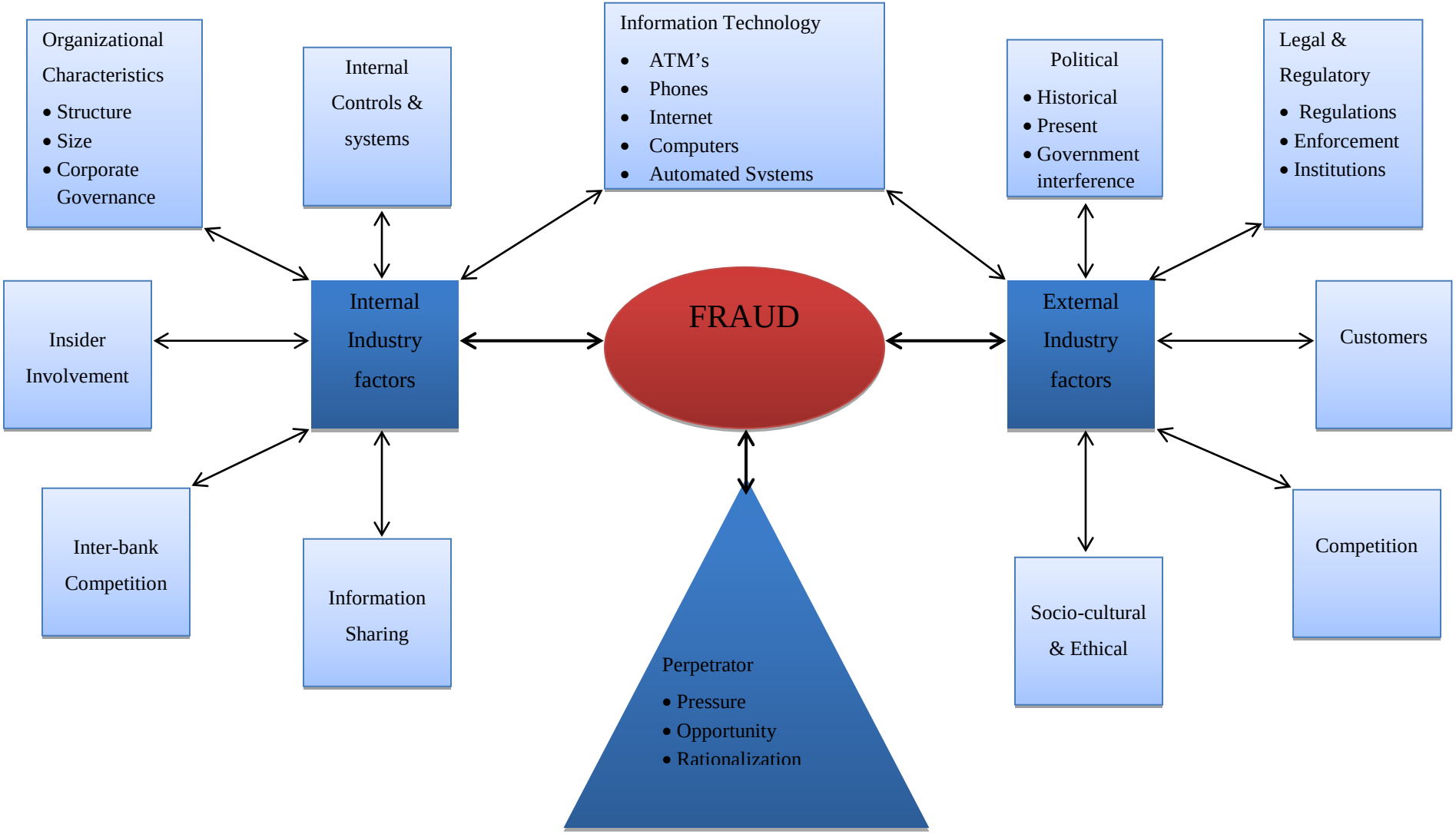


Figure 3.2: Conceptual Framework for fraud in Kenya's banking industry

3.10.1 The Fraud Triangle

The centre of the fraud is the fraud triangle representing the individual, which has been discussed earlier in Chapter 2, Section 2.3.1, as this model best describes the reasoning behind individual fraud and fraudsters.

The use of the fraud triangle as the foundational model can be justified by the fact that it has gained professional acceptance and this framework has been formally adopted into the Statement on Auditing Standards (SAS) No. 99 as an official model in detection of financial statement fraud (Ramos, 2003; AICPA, 2002). Table 3.2 operationally defines each of the three main elements.

Table 3.2 Definitions of individual factors in fraud (Fraud Triangle)

Factor	Definition
Pressure *(Section 2.3.1)*	Pressure will be defined as motivation for commission of fraud, which is defined as the non-sharable problem at the source of the fraud (Cressey, 1973; Wells, 2005). Six non-shareable problems (sub-types) leading to pressure to commit fraud will be included in this model. However, these sub-types should not be considered to be mutually exclusive, as they often interact (Cressey, 1973). • *Violation of obligations* will refer to pressure created from failure to meet obligations caused by gambling, drinking, drugs, or excessive personal debt (Wells, 2005). • *Personal failures* will refer to failure of investments, losses caused by bad judgment, divorce or other relationship failure (Wells, 2005) • *Business reversal* will refer to failures of business that cause pressure for fraud, including increase in business rates, losses due to recession, or other financial factors (Wells, 2005) • *Isolation* will refer to feelings that there is no one to share the problems with, including isolation at work as well as at home and in social life (Wells, 2005) • *Status gaining* will refer to behaviours that are focused on increasing the lifestyle status of the individual and allowing them to live beyond their means, such as purchase of luxury goods, houses, vehicles, or other high-status products (Wells, 2005) • *Employer-employee relations* will refer to behaviours promoted by a perceived breakdown of the relationship between the employer and the employee and feelings of betrayal or lack of trust resulting from this relationship breakdown (Wells, 2005).
Opportunity *(Section 2.3.1)*	*Opportunity* refers to the access and technical skills required in order to allow the individual to conceive of and successfully complete the conceived fraud (Cressey, 1973; Wells, 2005).
Rationalization *(Section 2.3.1)*	*Rationalization* refers to the a priori reasoning that the person committing fraud uses in order to allow them to commit the fraud and still maintain a personal image of himself or herself as an honourable person (Wells, 2005).

3.10.2 Industry Factors

Although the individual commits the fraud under the individual fraud triangle model described above, the fraud is not committed in a vacuum. Instead, there are significant elements of the banking industry that will influence whether fraud is committed and, if so, how it is committed. Thus, the second aspect of the conceptual analysis that will be examined is the internal industry (banking) factors that define the internal environment that enables fraud to flourish in the banking industry.

Internal industry factors include the following:

- Information sharing
- Competition
- Organisational characteristics
- Internal controls
- Insider involvement
- Information technology

Each of these factors is related to the ability of the banks to detect and prevent fraud within the environment of their own bank, including both positive and negative factors. Table 3.3 provides a definition of each of these variables, along with relevant sections of the literature review for further reference.

Table 3.3 Industry-level factors in fraud

Factor	Definition
Information Sharing *(Section 2.4.1)*	*Information sharing* will be defined as provision of information regarding customers, employees, and fraud mechanisms that is relevant to fraud prevention (Barth et al., 2008). Sharing information between banks in regard to customers, employees, and fraud mechanisms provides a protective mechanism within the banking industry as a whole as well as to individual banks that engage in the practice, as it allows for early identification of potential corruption (Barth et al., 2008).
Competition *(Section 2.4.1.3)*	*Competition* will be defined as the practice of seeking to attract customers from other banks and increase the bank's share of churn from individuals switching account. Increasing competition between banks can increase transparency (Barth et al., 2008).
Organisational characteristics *(Sections 2.4.2.1)*	Organisational characteristics include public, private, government, not for profit structures; size of the organisation is based on number of employees; revenue – for publicly trading organisations; internal controls – background checks, internal and external audits, anonymous reporting (Holtfreter, 2005; Smigel, 1956). Corporate governance, or the management of the bank in order to meet the needs of the appropriate group of individuals, is at the foundation of the need for fraud prevention (Macey & O'Hara, 2003). Issues in corporate governance include separation of ownership and control (Macey & O'Hara, 2003). However, research on corporate governance in the banking industry in Africa and other developing regions

	is rare (Arun & Turner, 20020 Lin, 2005; Prowse, 1997; Oman, 2001). Thus, this will not be considered strongly in this research.
Insider involvement *(Sections 2.2.2.1, 2.4.2.3.1)*	Insider involvement will be defined as a conspiracy between two or more parties in order to commit fraud, primarily through collusion by members of the organisation Breuer, 2006; Canhoto & Backhouse, 2007). Insider involvement can include self-dealing, embezzlement, insider trading, corruption and other forms, and is commonly discussed in the literature (Arun, 2008; Barth et al., 2008; Beasley, 1996; Beck, Demirguc-Kunt, & Levine, 2006; Black, 2005a; Black, 2005b; Cloninger & Waller, 2000; Crutchley, Jensen, & Marshall, 2007; Dixon, Ritchie, & Siwale, 2007; Dunn, 2004; Lee, Clarke & Dean, 2008; Pontell, 2005; Rezaee, 2005; Shen & Chih, 2005; Summers & Sweeney, 1998; Szockyj & Geis, 2002; Zahra, Priem, & Rasheed, 2007).
Internal Controls (*Section 2.4.2.3.1, 2.4.2.3.2*)	*Internal Controls* will be defined as procedures and checks and balances used within the bank to detect and prevent fraud (Wells, 2005). Internal controls are intended to be effective, but will not be effective in preventing control fraud or other endemic frauds within the organisation (Cressey, 1973; Wells, 2004).
Information Technology (IT) (*Section 2.4.1.2*)	As can be seen from the conceptual framework (Figure 3.2) information technology is both an internal and external banking factor Arnfield, 2004; Bierstaker, Brody, & Pacini, 2006; Bolton & Hand, 2002; Debreceny et al., 2005; Durtschi, Hillison, & Pacini, 2004; Edge & Sampaio, 2009; Fernandez & Gonzales, 2005; Homazi & Giles, 2004; Mannan & Van Oorschot, 2009; Paliwal & Kumar; Phua, Alahakoon & Lee, 2004; Phua, Lee, Smith Gayler, 2005; Sardanis, 2007; Shao, 1999).

These factors cannot be neatly divided into factors specific to individual banks or the general industry for obvious reasons; for example, most banks will have a limited range of internal controls that they can use, due to the regulation of the banking industry (Riahi-Belkaoui & Picur, 2000). However, banking regulations can often be too weak to create any significant change in the development of internal controls (Riahi-Belkaoui & Picur, 2000). Internal controls, organisational characteristics and insider involvement have been considered to be bank specific factors, while competition for customers and information sharing as industry-wide factors. Figure 3.3 shows the balance of these factors within this model.

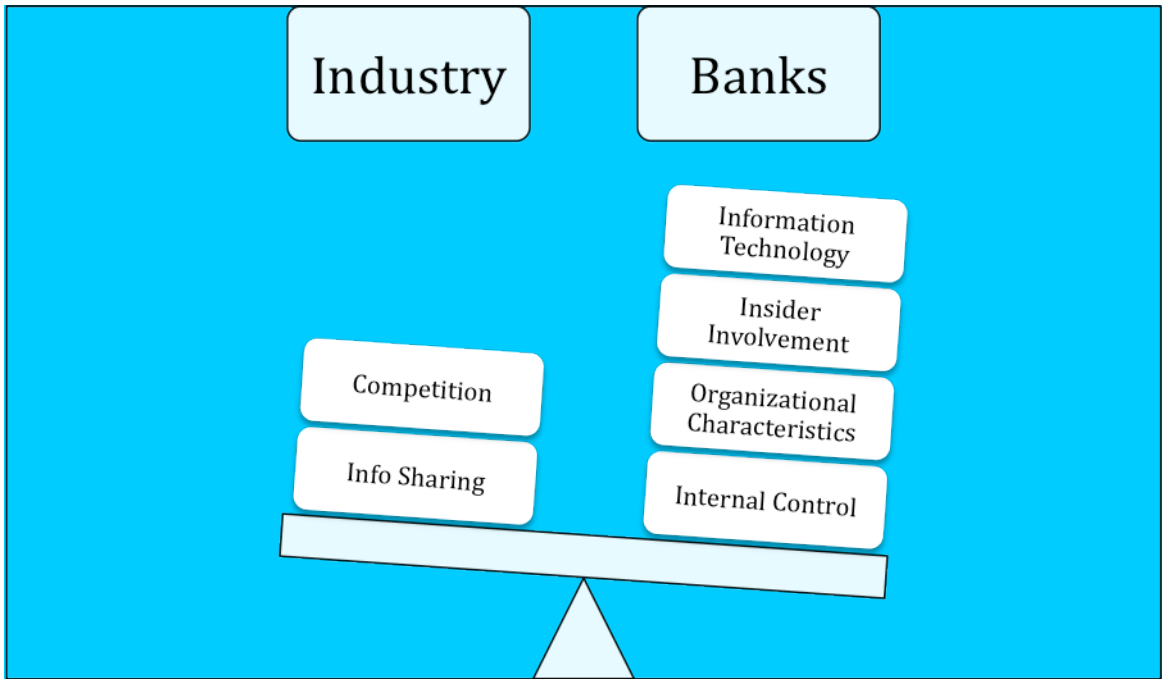


Figure 3.3 Industry and banking factors in the conceptual model of fraud

3.10.3 The External Industry Environment

The external environment around the banking industry is the third aspect of the conceptual framework. The individual sub-dimensions of the external environment include legal, ethical, socio-cultural, economic, political, information technology and the customer dimensions.

The external environment model can be visualized as shown in Figure 3.4. Table 3.4 provides a comprehensive definition for each of these factors in the external environment, which are not strictly ordered and which may influence each other.

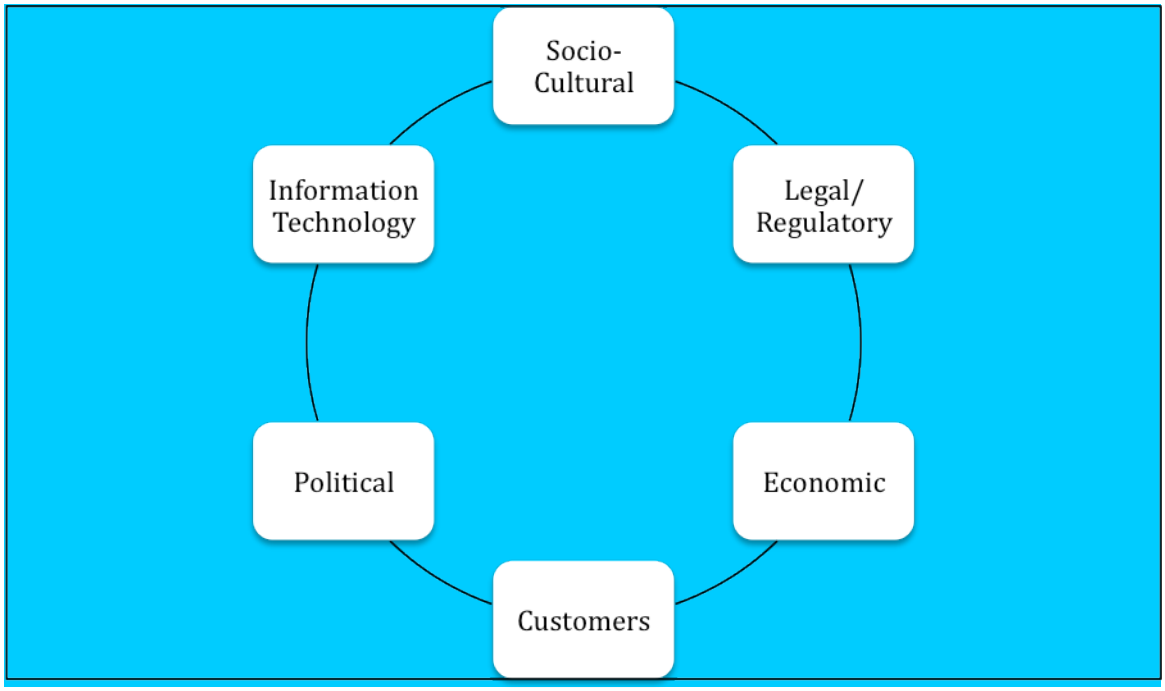


Figure 3.4 the external environmental level of the conceptual framework

Table 3.4 Definition of external environmental factors for the conceptual framework

Factor	Definition
Legal *(Sections 2.4.1.4; 3.7; 3.8)*	Legal can refer to laws, regulations, rules, and enforcement of these legal structures by government officials in the country of practice (Aguilar, Gill & Pino, 2000). The legal external environment will include factors such as regulation and regulatory bodies, corporate governance rules, law enforcement and prosecution of alleged perpetrators of fraud at the local, national, and international level (Macey & O'Hara, 2003). Some of the areas of the legal environment that may affect the outcomes of fraud management include the legal environment for lending (Barth et al., 2008), development law and corruption (Doidge, Karolyi, & Stulz, 2007), regulation of the corporate governance environment (Licht, Goldschmidt, & Schwartz, 2005), and availability, commonality and competence of police investigation and criminal prosecution (Wilhelm, 2004).
Ethical *(Sections 2.4.1.6)*	Ethical factors in the external environment can be defined as individual and cultural social norms and values that are internalized by the individual and provide guidance regarding the acceptance of fraud (Aguilar, Gill, & Pino, 2000). However, ethical values can at times be twisted in order to provide a rationalization for the use of fraud (Cressey, 1973; Wells, 2005). Ethical factors can be inculcated in the employee workforce of the bank through the use of ethical training (Aguilar, Gill, & Pino, 2000), as well as the use of whistle-blower programs in order to encourage the report of ethical issues within the organisation (Schmidt, 2005).
Socio-cultural *(Section 2.4.1.6)*	Socio-cultural factors will be defined as those factors that exist primarily in the social and cultural environment. Some examples will include the overall level of perception of corruption in the business environment (Bakre, 2007; Transparency International, 2009) and what is considered to be acceptable business practice (Zahra, Priem, & Rasheed, 2007).
Information Technology	Information Technology will be defined as the use of computer data storage and analysis technologies for internal control and the prevention and detection of fraud (Fernandez &

(Sections 2.4.1.2)	Gonzales, 2005). Information technology systems are commonly used in the accounting and auditing functions of banks, as well as in customer account management, connections with external agencies, other banks, and centralized banking systems, and other connections and analysis tasks (Fernandez & Gonzales, 2005). Information Technology can be a positive factor in detection and prevention of fraud (Fernandez & Gonzales, 2005). However, it is also highly vulnerable to inefficiency and ineffectiveness if the information technology is not implemented properly (Fernandez & Gonzales, 2005).
Political *(Sections 2.4.1.7; 3.4*)	The political environment will be defined by the history and role of the government intervention in the affairs of banks through politicians as it relates to the laws, agencies and other factors that are applied by the government.
Economic *(Sections 2.4.1.1, 3.5; 3.6;3.7)*	The economic environment will be defined by macro-economic factors that influence the banking industry in Kenya such as the banking crisis, moral hazard, adverse selection and corruption
Customer *(Section 2.4.1.5; 2.2.1)*	This will be defined as an individual or organisation that avails of the products and services offered by a bank and who maintain an account in the said bank.

3.10.4 Use of the Conceptual Model

This conceptual model will be used as a means of discussing fraud and formulating an understanding of what can often be a complex issue. The conceptual framework has been used in creation of the survey and interviews conducted in the study, and will also be used in discussion of the results of the survey and the interviews. This model will also provide a means of analysing the outcomes in terms of the existing literature and comparison of the findings to what have been identified as the most important factors in conduct of fraud. The conceptual framework, however, is descriptive of the expected findings of the research, rather than prescriptive; it is possible that other elements of fraud will be identified that are not included in this model, in which case they will be analysed in order to determine why they were not found in the existing literature.

3.11 Summary

This chapter has outlined a basic background of the banking industry in Kenya contextualizing it in relation to its historic, political, economic, legal and regulatory environments. These environments form an important part of the conceptual framework. The interaction of these environments helps to partly explain the nature and enhance the understanding of fraud in the banking industry. Kenya's banking industry has undergone several changes over the past two to three decades that have resulted in mergers, conversions and lately acquisitions. As a consequence the banking structure has

constantly changed. The first wave of the banking crisis in the 1980's was occasioned by poor management, weak internal controls, bad governance, insider lending especially to political banks resulting in non-performing loans and all catalysed by a weak legal, regulatory, supervisory and policy banking framework. The second wave of the banking crisis in the 1990's was precipitated by difficult economic and political reforms and the revelation of the Goldenberg scandal. Recent developments in information technology, new banking models, laws and regulations and information sharing have improved conditions in Kenyan banking. What remains clear is that historical events (both pre and post-independence) have contributed to fraudulent practices in the banking industry. Government interference and political influences have negatively affected the fight against fraud and corruption in the banking industry. The dynamic changes in the structure of the banking industry, regional expansion, new developments in ICT and new modes of financial service delivery to the customer all provide more challenges to fraud and risk management. However, the banking industry, through measures like credit referencing and devising new legislature, endeavours to provide sharing of credit information and to improve laws and regulation that can have a positive impact on the management and reduction of fraud.

Chapter 4
Research Methodology

4.1 Introduction

This chapter discusses the ontological and epistemological positions, methodology and methods used in the research design of this study. Ontology addresses the nature of being and reality, defining what is real in the world. The ontological position of constructionism was adopted for this study. This research further used a theoretical perspective that combined a positivist and interpretivist research philosophy in order to come to conclusions about the research topic. Subsequently, a triangulated research design that combined qualitative and quantitative methods of a questionnaire and interviews in order to examine the research questions is adopted. This chapter attempts to justify the methods applied in the research. The research methodology is focused on addressing the following research questions:

1. What are the characteristics of fraud in the Kenyan banking industry?
2. What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?
3. How do banks approach fraud management?
4. Are there differences between the approaches to fraud management adopted by Kenyan and international banks?

It also discusses various aspects of the research methodology including research approach (Section 4.2); research design and sample selection (Section 4.3); quantitative and qualitative research procedures (Sections 4.4 and 4.5); data integration and presentation (Sections 4.6 and 4.7); and various research issues including reliability, validity, generalisation, and ethics (Section 4.8). Section 4.9 concludes with general field reflections of this study.

4.2 Research Approach

Justification of the choice and use of specific methodology and methods is not only based on the research questions of the study but on the assumptions that we make about reality, our theoretical perspectives. Theoretical perspectives lie behind the choice of methodology and reflect the philosophical stance that informs this choice. Our theoretical assumptions reflect what we understand about human knowledge and what it entails. Theoretical perspectives on the other hand are informed by epistemology and ontology (Crotty, 1998). Therefore as shown by Figure 4.1 the methods proposed to be used in this study are governed by the methodology which in turn is influenced by the theoretical perspectives which are subsequently informed by the epistemology or ontology.

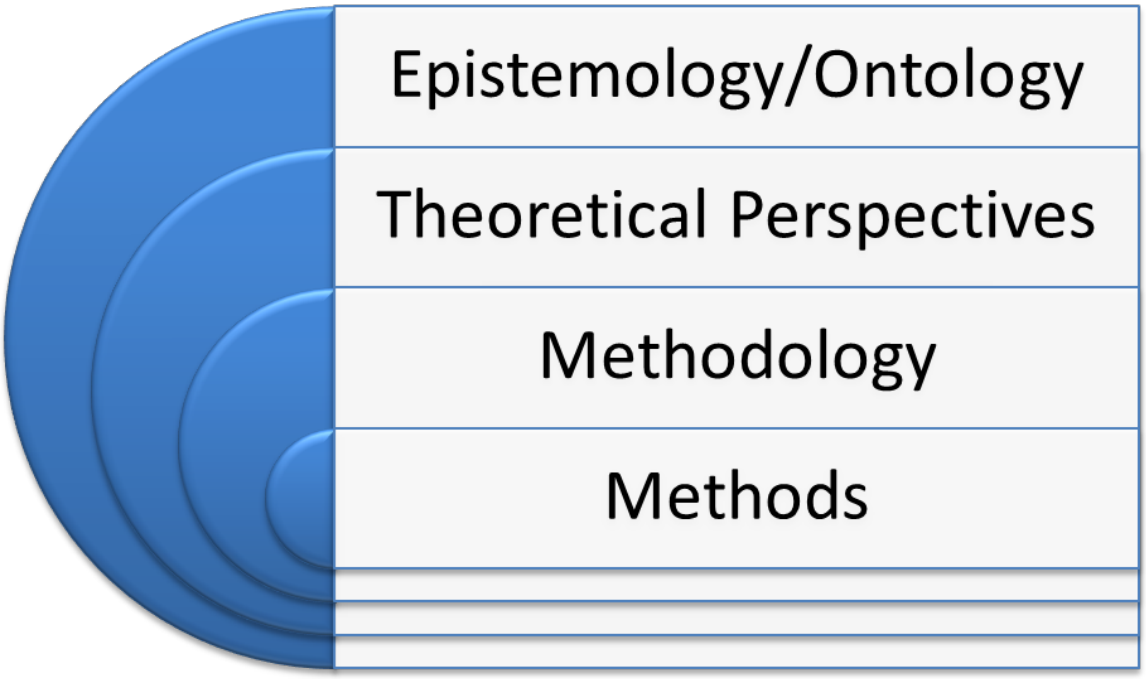


Figure 4.1: Four Elements of the Research Process

4.2.1 Epistemological and Ontological Position

According to Crotty (1998, p.10) “each theoretical perspective embodies a certain way of understanding *what is* (ontology) as well as a certain way of understanding *what it means to know* (epistemology).” Ontology is concerned with the nature of existence, the structure of reality. Epistemology deals with the nature, possibility, scope and general

basis of knowledge (Hamlyn, 1995) and "is concerned with providing a philosophical grounding for deciding what kinds of knowledge are possible and how we can ensure that they are both adequate and legitimate" (Maynard, 1994, p.10). Even though a fine line is drawn between epistemology and ontology the two concepts tend to be spoken of inter-changeably by several authors. This is because epistemological and ontological issues tend to emerge simultaneously. In order to construct meaningful reality there must be meaning and there must be meaningful reality to create meaning. Due to this confluence, writers have a problem in separating these two concepts (Guba and Lincoln, 1994; Crotty, 1998). Therefore in the research approach adopted for this study the terms epistemology and ontology will be used inter-changeably.

There are several possible epistemological/ontological stances that can be used in research. However, the three main epistemological positions are: objectivism, constructivism and subjectivism. Objectivist epistemology sustains that things exist as meaningful entities independently of consciousness and experiences. In other words, truth and meaning reside within and are found in the objects. Thus, "meaningful reality exists as such apart from any consciousness" (Crotty, 1998, p.8) and as illustrated by Crotty (1998) a tree in the forest is a tree irrespective of whether any one knows about its existence. When people recognize the tree they merely discover a meaning that was waiting to be discovered all along. Just like the source of the River Nile is Lake Victoria, even upon its discovery, Lake Victoria (object) had been lying there all the time waiting to be 'discovered'. Therefore under this ontological position, the objective truth can be uncovered because understandings and values are objectified in the people being studied.

The second epistemological/ontological position, constructionism, rejects the objectivists' view of human knowledge positing that there is no objective truth out there waiting for us to discover it. Therefore meaning is not discovered, but constructed (Crotty, 1998). As meaning is constructed and not discovered then different people construct meaning in different ways in relation to the same phenomena. This can be seen as you move from one generation to another, one culture to another, one time period to another. Thus, the

constructionist view is that the subject and object emerge together in the generation of meaning, which is a consequence of the mind and cannot exist without it.

The third epistemological/ontological stance is subjectivism, a variant of constructionism which is the view that meaning is created out of nothing, which is difficult considering that few human beings are creative enough, though it can be argued that we can learn from others' created meaning. Even in subjectivism, meaning must come from something, a dream, a religious belief or a voice in the subconscious. The point here being that meaning is imported from somewhere else and literally imposed onto the object by the subject rather than coming from an interaction between subject and object as in constructivism. In other words the object does not contribute at all in creating meaning (Crotty, 1998).

This study seeks to understand the nature and characteristics of fraud and how banks individually and collectively (based on type of bank – local, national, regional or international) approach fraud management. Different respondents will hold different perceptions of fraud and will construct different meanings of the same phenomenon that is, fraud, based on their fraud experiences with perpetrators and specific external and internal bank environments. Their perceptions of fraud may be dependent on but distinct from these factors. Therefore the ontological position chosen for this research is that of constructionism. As such, and as discussed above, this research cannot expose an objective truth independent to any consciousness, as would strictly happen under positivism, but it will explore a way of seeing things through the human eye of understanding as would occur under interpretivism (Crotty, 1998).

However, if the researcher were to treat epistemology and ontology on a separate footing then the epistemology of the study would be constructionism while realism would be adopted as the ontological position. Realism is an ontological notion asserting that reality exists outside the mind implying that the world and things in it exist independently of our consciousness of them. In this study it means that fraud exists whether we are conscious of it or not.

It is important to point out that some authors (Guba and Lincoln, 1994; Macquarrie, 1973) link realism as an ontological approach with objectivism in epistemology, an incompatible link. Crotty (1998, p.11) challenges this traditional link and observes that "realism in ontology and constructionism in epistemology turn out to be quite compatible". While agreeing that there is a world independent of the consciousness Crotty (1998) contends that the world without a mind in inconceivable and meaning without a mind is not meaning. This research can therefore comfortably adopt realism in ontology and constructionism in epistemology and remain compatible.

4.2.2 Theoretical Perspectives

As discussed at the beginning of Section 4.2 the theoretical perspective is the philosophical stance that informs the methodology chosen for a piece of research. The theoretical perspective provides grounding of the logic and criteria behind the methodology. Therefore, the theoretical perspective or research philosophy adopted will give rise to a number of assumptions that will subsequently influence the methodology (Crotty, 1998).

The research philosophy is important because it provides a foundation for the selection of research approach and design as well as a means to interpret or view the findings in regard to their context in the world.

There is a long- standing ontological and epistemological discussion on the best approach to adopt when conducting research. At the centre of this discussion are two different research inquiry approaches, namely the positivist inquiry, which typically employs experimental and quantitative approaches and the interpretive inquiry, which usually makes use of naturalistic and qualitative approaches to inductively and holistically understand human experience in context-specific settings (Patton, 1990). Even though a number of authors have engaged in the discussion and review of this debate (Cook and Reichardt, 1979; Patton, 1986; Fetterman, 1988; Lincoln and Guba, 1985; Denzin & Lincoln, 2003) there still remains a significant blur between the two research styles.

Rather than choosing one style of inquiry over the other Patton (1990) is in favour of a paradigm of choices. A paradigm is a worldview or "a cluster of beliefs and dictates which for scientists in a particular discipline influence what should be studied, how research should be done, how results should be interpreted, and so on" (Bryman, 1988, p.4). Patton (1990) argues that a paradigm of choices rejects methodological orthodoxy in favour of methodological appropriateness as the primary criterion for judging methodological quality. The issue therefore is not whether one has uniformly adhered to logical-positivist or interpretative canons but whether one has made a sensible methodological decision given the purpose of the inquiry and the research questions being investigated.

Bryman (1989, p.248) says that the "distinction between quantitative and qualitative research is not simply a matter of different approaches to the research process, each with its own cluster of research methods….but it concerns antagonistic views about more fundamental issues to do with the nature of one's subject matter." Therefore instead of viewing the interpretivist inquiry and positivist inquiry as competing approaches one should draw from both of them depending on the nature of the study. This research was conducted from a dual research philosophy of positivism and interpretivism, with each philosophy playing an important role in the outcomes of the research as well as its design. The next four sections discuss the theoretical perspectives and the mixed approach adopted in this study.

4.2.2.1 Positivist research inquiry

The first research approach that has been selected is positivism, most specifically the post-positivist approach of critical realism. Positivism is the foundational theory of the scientific method. It holds that the physical world and world of perception can be objectively measured and cause and effect can be described and identified with certainty (Schutt, 2003). This philosophy is foundational in quantitative research particularly, which focuses on the use of statistical connections between phenomena as measured and

observed. The positivist philosophy requires careful and consistent research design based on logical assumptions and the use of valid statistical measurement and comparison in order to lead to thoughtful and careful conclusions (Trochim & O'Donnelly, 2006). Positivists seek to explain the world by developing general laws that arise from what can be observed as facts (Henn, Weinstein and Foard, 2009). Thus, the positivist philosophy is highly suitable for statistical research work, as well as for the determination of cause and effect relationships.

Under the positivist inquiry the phenomena being studied is first observed, then theories are developed based on these observations. Through a continuous process of verification and observations of similar phenomena, positivists will develop a theory that later becomes a law which can be generalized to similar phenomena. Ironically the continuous verification-observation process that defines the positivist inquiry is also its drawback as it limits the progress of knowledge and there could be limitations based on observation. Thus Popper (1959, as cited by Henn, Weinstein and Foard, 2009, p.13) states the solution to these two problems lies *"not in attempting to verify what we already know, but in trying to falsify it."* In so doing theories can be tested against new data and should the data refute the established theory its general application can be challenged. Nonetheless, in this research what can be tested could be limited considering that fraud is a complex problem and it is elusive by nature. It can be difficult to accurately test aspects of fraud.

However, the positivist approach eschews any possibility that the researcher or respondents may introduce bias into the research (Schutt, 2003). This assumption is highly unlikely, in the view of this researcher, especially in regard to the controversial issue of banking fraud. Thus, a post-positivist approach was selected in order to allow for the possibility of researcher and response bias (Trochim & O'Donnelly, 2006). In this perspective, it is acknowledged that there are objective, external facts that can be observed and measured, and that these objective, external facts lend themselves to the methods of scientific inquiry (Grix, 2004). However, there is also an acknowledgement that in any form of social inquiry, the existence of objective facts does not preclude the potential that human interactions and interpretations play a significant role in constructing

subjective truth (Grix, 2004). Thus, in this theoretical perspective, there is no conflict between acknowledging the existence of objective facts and considering the potential for social construction of knowledge and reality.

The specific approach that was selected was critical realism, which philosophizes that it is not possible for human research to be completely free of bias; instead, the potential sources of bias must be carefully examined and isolated, as well as controlled in as much detail as possible (Fleetwood, 1999). The role of critical realism is to state that all theory can be revised, based on new research or new findings, and that the researcher will be inherently biased based on their interest in the subject (Trochim & O'Donnelly, 2006). Thus, the critical realism philosophy allows for the use of positivist rigor in the research while still allowing for the potential of human bias and the potential that previous research is flawed (Trochim & O'Donnelly, 2006). This demands re-examination of the research material based on new findings and outcomes. This approach is widely used in the field of economics, in which purely financial or statistical information must be combined with information regarding the motivations of the researcher and the participants (Fleetwood, 1999).

Unlike the qualitative approach that works best with small samples, is relatively unstructured and based upon descriptions, the quantitative approach is suited for a study that has a relatively large sample, is highly structured and based on statistics. Qualitative researchers believe that rich descriptions of the social world are valuable whereas quantitative researchers' believe that such detail interrupts the process of developing generalizations (Denzin & Lincoln, 2003, p.16). For the positivist precision, objectivity and rigor replace hunches, experience and intuition as the means of investigating research problems, and consequently social science is based on the approach used in the natural sciences. (Colins and Hussey, 2003, p.52) Even though the use of quantitative tools, like the questionnaire, under the positivist approach restricts participants to only what has been asked, greatly limiting their views and opinions, it still has its benefits. One benefit of using quantitative data is that it can measure the reaction of many people to a restricted set of questions facilitating comparisons and allowing for findings to be generalized (Patton, 1990)

4.2.2.2 Interpretive research inquiry

The goal of the researcher was not merely to explain the specific relationships between variables studied, but to consider what these relationships *meant* in the context of the Kenyan banking industry on the whole. However, positivist philosophy does not allow for the kind of interpretation required to support the research demands. Thus, the researcher used a dual research philosophy, including interpretivism in the research philosophy in order to provide a more balanced design. Interpretivism is a wide-ranging group of research philosophies, which is often viewed as the opposite or antithesis of the positivist approach. Interpretivist approaches are useful in the social world, and are based in the assumption that humans, and research derived from them, is inherently subjective (Grix, 2004).

Qualitative data provide an avenue to establish well grounded, rich descriptions and fruitful explanations of processes in identifiable local contexts. Such data can also give rise to unexpected findings and new relationships useful in confirming or revising conceptual frameworks (Miles and Huberman, 1994). Interpretive research inquiry emphasises an attempt to understand social phenomena by constructing meaning from actual lived experiences of participants in the research. Hence an individual's experience is best explained and understood from their own perspective or world view. Interpretivists seek to understand how people attribute meaning to their circumstances. In the words of Denzin and Lincoln (2003, p.13) qualitative researchers' stress the socially constructed nature of reality, the intimate relationship between the researcher and what is studied – they seek answers to questions that stress how social experience is created and given meaning. In this research using qualitative inquiry allows the interview participants to present their opinions and views on fraud in the banking industry, allowing their views to take precedence over those of the researcher. By listening to their fraud experiences the researcher is able to pick out the key words in the comments and responses made by the participants. Words, as described by Miles and Huberman (1994), *"especially organized into incidents or stories, have a concrete, vivid, meaningful flavour that often proves far more convincing to a reader – another researcher, a policymaker, a practitioner – than pages of summarized numbers."* In the interpretative inquiry participants are allowed to

explain their world in their own words and as Henn, Weinstein and Foard (2009, p.16) suggest “Language is considered a tool with which we make meanings.”

Thus in an interpretive research approach the participants are active, portraying inner capabilities which allow for individual perceptions and judgements, and are not merely passive vehicles in the matter under research. They can influence, change and contribute to meanings. Blumer (1969) suggests that a distinct feature of human reaction is that it is not based on people reacting to each other rather it is based on people interpreting each other’s actions. Therefore interpretive research involves researching ‘with’ and not ‘on’ people. Henn, Weinsten and Foard (2009, p.15) state that “human action can only be understood by relating it to the conscious intentions, motives, and purposes and ultimately the values of the agent that performs it.”

Thus interpretivists argue that social realities lie in what people do, say and think, rather than the kind of abstract system that is somewhat greater than the sum of its parts as advocated under the positivist inquiry (Garrick, 1999). How a researcher carries out their research is influenced by the general interpretivist assumptions and the philosophical issues underpinning the study and by weaving together an understanding we are finally able to build rather than test a theory (Henn, Weinstein and Foard, 2009).

According to those who support the interpretivist inquiry there are no absolute answers (Candy, 1991; Mezirow, 1996) as there are alternative ways of understanding social phenomena. Thus they also argue that due to the diversity of social reality, how it is known, experienced and constructed, social theories cannot be generalized universally as they are specific to given cultural and historic set ups (Denzin and Lincoln, 1994). Given that interpretivists regard the research process as an interaction between two or more people the researcher and the participant become players. According to Patton (1990, p.14) “in qualitative inquiry, the researcher is the instrument.” This is supported by Brannen (1994), who says that researchers must use themselves as the instrument.

This makes the interpretivist inquiry appropriate for some of the issues being studied in this research. An interpretive approach considers and acknowledges the processes by which the individual makes sense of their world. It also allows for the researcher's role in knowledge construction to become more explicit. Given the sensitive, broad and complex nature of fraud issues interpretive research inquiry is relevant and suitable for this study. Fraud has also not been widely studied academically in Kenya's banking industry making it an under-developed research topic. The interpretivist inquiry can be best applied to explore or build up an understanding of something, which in our case is fraud, of which there exists little knowledge (Henn, Weinstein and Foard, 2009). It is also an area where existing theory suggests the use of or making up of narratives may be anticipated; for example, the fraud triangle on one part consists of rationalization.

4.2.2.3 The mixed approach

Interpretivism is based on a number of specific differences from positivism, including a belief in the social construction of views by people, and the role of the social world in influencing human action. In direct contrast to the positivist approach, the interpretivist approach does not assume the existence of a social world independent of the observation of its participants (Grix, 2004). The ultimate conclusion of this position is that value-free or objective research is simply *not possible* in the social world, and as such is inappropriate for social research in general and perhaps no less in fraud studies.

While the interpretivist inquiry is an analytic-inductive approach and the positivist inquiry is largely a hypothetical-deductive approach, an evaluation can include elements of both inquiries (Patton, 1990, p.46). Table 4.1 summarises the distinction between quantitative and qualitative paradigms.

Table 4.1 Distinction between interpretivist and positivist paradigms

	Interpretivist	**Positivist**
Basic beliefs	• The world is socially constructed and subjective • The observer is part of what is observed • Science is driven by human interest	• The world is external and objective • The observer is independent • Science is value- free
Researchers should	• Focus on meaning • Try to understand what is happening • Look at the totality of each situation	• Focus on facts • Look for causality and fundamental laws • Reduce phenomenon to the simplest elements • Formulate and test hypotheses
Preferred methods	• Develop ideas through induction from evidence • Small samples investigation in depth or over time.	• Operationalize concepts so they can be measured • Large samples

(Source: Remenyi et al, 1998, p. 104)

4.2.2.4 Triangulation and Integration of Research

Epistemological and theoretical positions have influenced the character of both quantitative and qualitative research. Quantitative research has been influenced by the natural science model of research and its positivist form while qualitative research has been influenced by an epistemological position that rejects the appropriateness of a natural science approach to the study of humans (Bryman, 1994; Brannen, 1994).

Research can be most fruitful when both the quantitative and qualitative research approaches are used (Bird, 1994) and the triangulation research design allows for consideration of research in two ways. The triangulation approach examines the research question from a qualitative and quantitative perspective separately (Creswell, 2009). The use of quantitative research allows for consideration of the research questions using a strictly positivist approach, identifying cause and effect through the use of statistical

analysis (Creswell, 2009). The use of a qualitative approach allows for the use of the interpretivist philosophy, in which the construction of the social world is considered to be a key influence on the research findings. Both approaches have their own strengths and weaknesses and this provides a good reason to combine them.

According to Bryman (1994, p.63), triangulation is drawn from the idea of "multiple operationism" which suggests that the validity of findings and the degree of confidence in them will be enhanced by the deployment of more than one approach to data collection. Moreover, Denzin and Lincoln (2003) suggest that triangulation reflects an attempt to secure an in-depth understanding of the phenomena in question. Citing Flick (1998), Denzin and Lincoln (2003) add that triangulation is not a tool or a strategy of validation, but an alternative to validation. They further state that the combination of methodological practices, empirical materials, perspectives and observers into one study is a strategy that adds rigor, breadth, complexity, richness and depth to any inquiry.

4.3 Research Design

The research design can be summarized as a mixed methods approach. The mixed methods approach to research examines a research problem from both a qualitative and a quantitative perspective, integrating findings from both approaches in order to arrive at a highly robust approach (Creswell & Plano Clark, 2007).

The mixed methods approach is intended to provide a robust research process that mitigates the weaknesses of qualitative and quantitative research individually. Qualitative research is often thought to be prone to bias, difficulty in interpretation, and difficulty in limitation of the findings (Creswell, 2009). On the other hand, quantitative research can be unnecessarily limited and may miss important issues in the research due to the perceptions of the researcher, as it does not allow for any additional input to be found. Thus, the combination of qualitative and quantitative research can provide substantially improved research due to the integration of both perspectives, allowing for the researcher to consider additional information while at the same time maintaining the statistical rigor of the quantitative approach (Creswell & Plano Clark, 2007). This allows for a more comprehensive research process.

Mixed methods research is not without its own weaknesses, although it does provide some balance for the weaknesses of each of the two combined methods. One weakness is the difficulty involved in integrating the research findings of both the qualitative and quantitative study. Another issue is how to identify the findings that are relevant to the specific research questions (Creswell & Plano Clark, 2007). Qualitative and quantitative research can both be used to generate substantial findings that are not strictly defined within the auspices of the research findings. However, by maintaining careful control of the research design, the researcher can reduce the potential that irrelevant findings will be included in the research. Finally, the mixed methods approach can at times be complex and require more resources and time to complete the research effectively.

The mixed methods approach was chosen as a means to provide both the statistical balance of the quantitative approach and the breadth and increased understanding of the research subject. It was also selected in order to overcome the difficulties involved in both the qualitative and quantitative research approaches. Neither of the two approaches was considered to be adequate for full consideration of the research questions, and thus the research would be most appropriately conducted under the mixed methods approach. The triangulation analysis approach was used in order to overcome the difficulty in integrating the results of the research.

The decision to combine approaches for a study should be guided by the research problem at hand. Needless to say that a research that combines the two approaches is not necessarily always superior. For this reason, the research methods adopted for this study will be triangulated. Johnson and Onwuegbuzie (2004) state that employing a pragmatic and balanced or pluralist position helps to improve communication among researchers from different paradigms as they attempt to advance knowledge (Maxcy, 2003; Watson, 1990) and to shed light on how research approaches can be mixed fruitfully (Hoshmand, 2003).

4.3.1 Sampling strategy

There are two types of sampling techniques, namely probability sampling and non-probability sampling. There is no hard and fast rule regarding when probability sampling can be employed. However, if it is important for the researcher to be able to generalize to a wider population then probability sampling would be the most appropriate sampling approach. Non-probability sampling would be suitable for a study whose research questions do not specify the unit of analysis, such as a particular category of people, that should be sampled (Bryman, 2004). Thus in probability sampling the people or units chosen as the sample will be representative of the whole population under study allowing generalizations to be made while in non-probability sampling the chosen sample may or may not be well representative of the wider population. Due care should therefore be made when selecting a sample for use with a non-probability sampling method to enhance the chances that the selected sample will be representative of the other units in the study. There is a greater preference by researchers to use probability sampling as it is deemed to yield verifiable accurate results compared to non-probability sampling. Probability sampling is also often more favoured under positivism. However, there are areas of study where it may not be practical or possible to use probability sampling. Lincoln and Guba (1985) describe non-probability sampling as being emergent and sequential. This arises from the nature of the research process, which depicts a journey of discovery as opposed to hypothesis testing.

In this study non-probability sampling, specifically purposive sampling was used to identify the initial respondents. Most qualitative samples tend to be purposive, rather than random (Miles and Hubermann, 1994). As the title implies purposive sampling is sampling with a *purpose* in mind. In this case specific pre-defined groups are usually identified at the beginning of the study as part of the sample. Non-probability sampling enables the researcher to select research participants that have the experiences necessary to understand the phenomena in question, which in the case of this study is fraud. By so doing it is possible to get the views and opinions of the target group, which are valuable.

Whenever fraud occurs there are a perpetrator and a victim. It would have been ideal to collect the views and opinions from perpetrators to get a good picture about their motivations and rationalizations. However, finding fraud perpetrators to interview would have been an uphill task. Moreover, the perpetrators were probably less likely to give truthful information about their actions and motivations. Thus a decision was made from the onset to purposely select respondents, first through established contacts and then subsequently through the snowballing technique, from among those who were knowledgeable about fraud and were involved in actively preventing and detecting fraud in the banking industry. This group represented key organisational staff such as internal auditors/managers, fraud investigators/managers, operational risk managers, information systems managers, security personnel, financial crime team members and forensic auditors among others. As stated by Krambia-Kapardis (2004) when surveying corporate victims of fraud it is essential to decide the appropriate person in the organisation to respond as failure to do so may lead to a low response rate. The choice of whom to talk with, where, when, about what, and why, places limits on the conclusions we finally draw and how confident others feel about them (Miles and Hubermann, 1994). By sampling people we can get at the characteristics of settings, events and processes. However, determining the appropriate person(s) as respondents can be hampered by practicalities, such as, being able to gain access to them.

Miles and Hubermann (1994) on the other hand point out that samples in qualitative studies are usually not wholly pre-specified, but can evolve once the fieldwork begins with the initial choice of informants leading the researcher to similar and different ones. For this study, after the initial group of respondents was purposely selected the researcher was able to identify more respondents recommended or introduced by those purposely selected. This introduced the use of snowball sampling. According to Patton (1990) snowball sampling identifies cases of interest from people who know people who know which cases are information-rich. Both a formal and informal network was exploited to find suitable respondents.

4.3.2 Population

Although individuals were used for sampling, the level of analysis for this research was the bank. The population of this study consisted of all the banks in Kenya. As discussed in the previous chapter (Section 3.1) the number of banks in the industry has changed with the Central Bank reporting a total of 45 banks in the years 2006, 2007 and 2008, a total of 46 banks in 2009 and 43 banks as at the end of 2010. At the time of data collection there were 45 banks and this was adopted as the population of the study.

4.3.3 Sample

The research was conducted at both an individual as well as organisational level with individuals representing their views as well as the views of the organisation. The sample consisted of 40 out of a total of 45 banking institutions. Five banks were excluded due to age (under five years) and organisational stability reasons.

Given the relatively small size of the industry and the potential size of the participant pool, it was necessary that the sampling strategy cover the entire industry. Encouragingly Emory and Copper (1991 p.248) states that "it is not true that the research is considered representative if it has a large sample area." However, given the sensitive nature of the research, the researcher did not set a specific number of participants in recognition of the fact that it may not be possible to meet a given number of participants. Nonetheless as a guide the researcher set out to reach two people (knowledgeable about fraud in the organization, such as auditors, fraud investigators, security managers etc.) in each one of the 40 sampled banks for the quantitative study (80 respondents) and one person in every two banks (20 respondents) for the interviewing process. Thus, the sampling strategy was to poll every potential participant in the study and seek permission for the study's engagement. This approach resulted in 60 out of the intended 80 respondents contacted for the quantitative study. The 60 respondents were senior and upper middle level managers as already defined in Section 4.3.1. All respondents were from head offices located in Nairobi. Views represented at least 70% of the market share controlled by the largest nine banks. For the qualitative part of the survey 17 senior managers agreed to

participate in semi-structured interviews. The research respondents were contacted in person, by telephone and via email.

The response rate was expected to be between 40% and 50%, which would translate into an adequate representation (Blumberg, Cooper and Schindler, 2005). The quantitative survey achieved a 75% response rate while the qualitative study reflected an 85% response rate. The high response rate was achieved through maintaining a simple questionnaire that was easy to follow, keeping the length of interviews short, notifying the respondents in advance of sending out the questionnaire or conducting the interviews, constant follow up of respondents and participants' interest in the research.

4.4 Quantitative Research Process

Primary data was collected by the use of a questionnaire and interviews. The reason for using these different tools lies in the fact that they are able to capture and verify sensitive issues (Mintzberg, 1983; Patton, 1990). This following section discusses the data collection and analysis in two parts to capture both the quantitative and qualitative approaches used.

The quantitative research process was based on a questionnaire distributed to the participants in the survey. The questionnaire contained structured questions with options for "other" to capture any new or unique information. It was administered to auditors, accountants and/or other managers that were knowledgeable about fraud in these organisations, such as electronic fraud managers and Information Systems Audit managers.

4.4.1 Instrument Design and Testing

The survey used a questionnaire consisting of 29 questions focusing on four different areas of concern, namely; the general view of the respondent toward banking fraud and its growth in the industry, details regarding a recent typical fraud uncovered by the bank, organisational responses to this fraud, and specific details regarding the respondent. This

instrument design was intended to support the research questions and hypotheses, and provide specific information into these processes.

The instrument was tested in two stages. A pre-testing stage involved independent review by three individuals that were familiar with the subject matter and with survey design and adjustment of the survey in order to account for the feedback provided by these details. The resulting instrument was then pilot tested using a total of fifteen volunteer respondents. These participants completed the survey, pointing out areas of difficulty with the survey. These included difficulty in understanding some questions, as well as areas where respondents could not provide information due to non-disclosure agreements or other industry issues. Almost all the participants felt that the questionnaire took a longer time to fill than they anticipated. However, they were of the opinion that the questionnaire was an appropriate tool to collect information about fraud in Kenya. They did confess that despite the length of the questionnaire, all questions were relevant and none of them should be deleted. Some of the participants in the pilot study were of the opinion that some of the question-answer categories should be condensed. The survey was then adjusted in order to account for the feedback of the pilot study group. The final version of the questionnaire is attached in Appendix IIIA

4.4.2 Data Collection

Before any data was collected ethical approval and clearance to proceed with the research was sought from the Ethical Approval Committee of the Graduate School in keeping with the code of research at the Nottingham Trent University.

The data collection process was conducted as follows. First, participants were given an overview of the research, informed consent forms, and institutional release forms in order to ensure that all data collected could be used in accordance with the requirements of human subjects' research. Participants were then sent the survey using email, postal mail, or by hand. Each participant was assigned a participant number in order to remove institutional names from any respondents. The researcher logged the responses from each respondent as they were returned, with the researcher logging each response and entering

it into the data set. The researcher followed up with non-responding participants at two weeks intervals. The researcher clarified missing or unclear responses by following up with respective participants by telephone and/or email. Barring a few participants most of them were easily accessible and willingly gave follow up contacts to the researcher. In total number of respondents were 60. As indicated earlier in Section 4.3.3 the estimated sample size for the quantitative survey was 80 respondents. The response rate for the survey was therefore 75% of 80 respondents.

4.4.3 Data Preparation

The data preparation process involved the creation of an SPSS data set from the responses of the survey. A data set was created from the final tested instrument in preparation for the research. As each response was collected, the researcher entered the responses to each item into the data set, including participant number in order to be able to double-check the responses. The researcher then had a second individual double-check the accuracy of the responses entered into the data set, in order to ensure accuracy. Any errors that were found were rectified and then double-checked. This preparation structure was intended so that the analysis could begin immediately on completion of the data collection process.

4.4.4 Data Analysis

The data analysis process was performed in SPSS. The data analysis included descriptive statistics created in SPSS for each variable. This was performed for two reasons. First, a respondent profile was created in order to describe the conditions under which the survey was constructed. Second, a complete descriptive statistical run was performed in order to understand the relative commonality of the responses. The analysis then used an inductive statistical technique, the Chi Square, in order to test whether a relationship exists between the variables indicated in the hypotheses. The specific statistical technique used in establishing relationships in each hypothesis is discussed in the next chapter. The confidence level used for analysis was 95% ($p < .05$). This allowed for 5% or less chance of Type I error.

4.4.5 Choice of Statistical Tests

The first set of statistical tests that were selected was descriptive statistics. Descriptive statistics are a way of presenting the characteristics of a given sample in terms of the frequency of occurrence of specific polled traits. Descriptive statistics, including counts and frequencies, measures of central tendency (such as mean, median, and mode), and measures of dispersion (such as standard deviation and range) that allow for the description of the distribution of the sample (Johnson & Bhattacharya, 2009). Another descriptive statistic, the odds ratio, was also used to describe the degree of independence and the chance of a given occurrence in a series of events (Moore & Notz, 2006).

There are some weaknesses with the descriptive approach, which led to the use of additional tests in order to fill in these gaps. Under ordinary conditions, descriptive statistics cannot be used to make generalizations to the full sample (Brase & Brase, 2007). However, in this particular instance that may not be the case, given that the sample was close to a census (or a survey of the entire population). However, this does not mean that descriptive statistics are entirely sufficient to the task of answering all the research questions involved (Trochim & Donnelly, 2006).

For testing the hypotheses the chi square test for differences in distribution was used. The chi square test for difference in distribution uses the chi square coefficient ($\chi 2$) to determine whether there is a difference from the actual and expected distribution. This can be performed using either a specified distribution or can assume equal distributions (Moore & Notz, 2006). The chi square test was used to compare distributions of categorical and nominal data characteristics and determine whether they were different from the expected distribution. As one of the few tests that can be used to compare the distributions of nominal and categorical data (Johnson & Bhattacharya, 2009), this was considered to be the appropriate choice.

Pearson's Chi-Square test was used to test the null hypothesis that the frequencies in the columns of a cross-tabulation were not significantly associated with the frequencies in the rows. The Pearson's Chi-Squared statistic (χ^2) was computed by SPSS using the

"Analyze - Descriptive Statistics - Crosstabs" menu option (Field, 2009). The χ^2 test statistic was interpreted to infer whether or not the probability (p-value) of an association between the frequencies in the rows and the columns of the cross-classification was due to random chance. The p-value could range from a minimum of just above 0 (a very slight chance that the data were caused by random chance) to a maximum of just less than 1 (a very high chance that the data were caused by random chance). The problem is how small does the p-value have to be before the H_0 can be rejected? The decision rule used in this study was to reject the null hypothesis if the p-value of the χ^2 test statistic was less than the conventional significance level of $\alpha = .05$. The value of α reflected the probability of the test producing a Type I error (i.e., the false rejection of the null hypothesis when, in fact, it should not be rejected). This limit was set to a small value, typically $\alpha = .05$, so that the probability of a Type I error was reduced. The use of $\alpha = .05$ implied a 1 in 20 chance of making a Type I error, which is conventionally agreed to be an acceptable level (Field, 2009). The limitation of all null hypothesis statistical tests, including the Chi-Square test, is that the test statistics and p-values are extremely sensitive to sample size. If the sample size is too small then there is an elevated probability of a Type II error (i.e., not rejecting the null hypothesis when, in fact, it should be rejected). If more than 50% of the cells in a cross-tabulation contain frequencies less than five, then the results of a Chi-Square test are invalid (Agresti, 2007). In order to ensure that the cells of each cross-tabulation in this study contained sufficient cases, the original categories used for the questionnaire items had to be judiciously collapsed (i.e., two or more existing categories containing less than five cases had to be combined together in order to create a new category containing more cases). Despite collapsing the categories, not all the cells in the cross-tabulations contained at least five cases.

Before conducting null hypothesis statistical tests it was essential to specify the measurement levels of each variable collected using the questionnaire, because different types of null hypothesis statistical tests in SPSS operate on different types of variable (Field, 2009). Interval/scale level variables are continuous measurements with an equal interval between each successive measurement. Ordinal level variables are grouped into

numerical categories, such that each category is ranked into logical order, from low to high, but the distance between each category is not equal. Nominal variables are grouped into qualitative categories which cannot be ranked into a numerical order. All the variables analysed in this study were measured at the ordinal or nominal level. SPSS required each ordinal or nominal level category to be coded with an integer, known as a value label. As all the variables were categorical, it was not possible to use parametric statistics (e.g., means and standard deviations) which assume normally distributed scale/interval level variables (i.e., their frequency distribution is a bell-shaped curve). Only non-parametric statistics appropriate for ordinal and nominal variables were justified.

4.5 Qualitative Research Process

The qualitative research process started after the first batch of 40 questionnaires were received and tentatively analysed. The preliminary analysis was useful in highlighting some emergent issues that could be followed up in the interviews. A total of 17 out of 20 participants agreed to participate in further research. The qualitative research process was interview-based, with a semi-guided interview process allowing for the researcher to gather specific information, while allowing participants to include further information.

4.5.1 Instrument Design

The instrument used in the interview process was a semi-guided interview guide, which included 30 qualitative questions based on the findings of the quantitative research as well as information from the literature review. These questions were put through the same pre-testing process as the quantitative research, with the interview questions being looked over by three subject matter experts who were familiar with the research structure. However, this instrument, in keeping with the qualitative structure, was not put through pilot testing. A copy of the interview schedule can be found in Appendix IIIB.

4.5.2 Data Collection

The data collection process involved personal visits to the participants. Interviews were all conducted in the capital city, Nairobi where all banks have their headquarters. The

researcher began with a discussion of the interview process, making sure that the participants understood the aims and objectives of the research. The participants were also informed about their right to withdraw from the research and encouraged to provide any additional information that they thought was of relevance during the course of the interview. Participants were also explained to about the importance of informed consent, anonymity and confidentiality. Each participant signed a consent form before the start of the interview. The researcher recorded the interviews in order to ensure that the full input from the participants could be available. Prior to beginning the interviews the researcher sought consent from the participants to have their interviews recorded. All participants agreed to be recorded and were willing to affirm it by signing the consent form. Interviews lasted typically between thirty to just over sixty minutes (excluding, introductions, exchange of pleasantries and final appreciations).

4.5.3 Data Preparation

Following each interview, the researcher transcribed the interviews as conducted, including research questions and the responses to these questions. A paper copy of each transcript was prepared in order to allow note taking and manual coding. A database was then prepared in order to allow for the paper coding to be more easily analysed, with sheets for each interview question.

4.5.4 Data Analysis

The data analysis process used an open coding process first, in order to create all possible codes for analysis. Saldana (2009, p.3) explains a code as "a word or short phrase that symbolically assigns a summative, salient, essence-capturing and/or evocative attribute for a portion of language-based or visual data."

Coding was based on content analysis, with the meanings of comments and answers rather than the specific words being used as the basis for the coding process in most cases. Focusing on each question, the researcher then identified the most common codes from each of the participants. These common codes were examined in light of the research questions, and were then constructed into a narrative framework that examined

these questions in detail. Coding was performed manually, due to familiarity with data and the relatively small size of the sample.

In discussing qualitative analysis, Miles and Huberman (1994) explained that in analysing data three stages are important; namely, data reduction, data display and conclusion drawing and verifying. Data reduction gives rise to three levels or categories of information: text driven categories, coherence-driven categories and theory driven categories. The interview data was transcribed and significant segments of texts and themes that relate to the conceptual framework were drawn out from the transcribed interviews. Text-driven categories were then formed with themes being extracted. An effort was then made to conceptualize logical links and relationships between the themes, giving rise to coherence-driven categories. Finally, a link was established between the coherence-driven categories and literature gathered to develop theory-driven constructs.

Data display involved taking the reduced data and displaying it in an organised, compressed way so that conclusions can be more easily drawn. Miles and Huberman (1994) state that conclusion drawing and verification is the final analytical activity for the qualitative researcher, through noticing patterns of differences and similarities, regularities and irregularities, explanations, casual flows and propositions.

Following the analysis, the researcher contacted the participants and offered them the opportunity to review the interpretation of the findings. (This was in order to enact the interpretivist philosophy, as well as the critical realist philosophy, in order to provide multiple points of view of the research and help to reduce the potential for researcher bias). There was no additional feedback to the original information provided. However, their affirmation of the analysis was a positive confirmation on the accuracy of the information.

4.6 Data Integration

A triangulation approach was used for integration. In this approach, the researcher used qualitative and quantitative findings to discuss and answer each of the research questions (Creswell, 2009). Each of the findings for the qualitative and quantitative research is presented separately. However, the hypothesis-proving efforts are only approached using quantitative research, because of the goal of hypothesis proving. The qualitative research is also used to expand the findings and discuss the views of the research participants that were not detected in the research.

4.7 Data Presentation

The data presentation is in three sections. First, a respondent profile was constructed that identifies the overall characteristics of the participants. Then, a section on the quantitative findings discussed the descriptive findings as well as the inductive analysis that was conducted. These sections are included in Chapter 5. Chapter 6 encompasses the findings of the qualitative research, while Chapter 7 discusses these findings in terms of their position within the existing literature, including how it meets the expectations set by the existing research as well as how it differs from these expectations. A variety of tables, graphs, and other representations are used in order to describe the findings.

4.8 Research Issues

The research issues that were encountered during this research process were important in determining the outcomes of the research. The main issues include reliability, validity, generalization of findings, and the ethics of the research process. Each of these issues is discussed in detail below. It should be noted that these issues do have some difference in meanings based on the qualitative and quantitative research, and each of these is discussed separately below.

4.8.1 Reliability

Scale reliability in quantitative-based studies is defined as the degree to which scale items are free from random error (McDaniel and Gates, 2007). It expresses the "ratio of the variance of the true score to the variance of the observed score" (Netemeyer et al,

2003, p. 42). Kerlinger (1973) argues that concepts that may be synonymous to reliability often demonstrate characteristics of "dependability, stability, consistency, predictability, and accuracy" (p. 442). Thus, reliable scales are those that can be depended on and that show consistency over time.

The particular concern for reliability in this instrument is internal consistency reliability, or the ability to ensure that items within the test are reflecting the same constructs (Trochim, 2006). There are different methods for assessing the reliability of a construct. However, a common research practice is to report coefficient alpha of all multi-item scales, whether these scales are borrowed from existing batteries or are newly developed or both.

Reliability in qualitative research is not based on the ability to re-measure results. Instead, this concept in critical research is based on issues like ontological appropriateness, multiple perceptions of participants and other researchers, and methodological trustworthiness (Healy & Perry, 2000). Although some researchers argue that reliability is a purely quantitative concept and there are no applications to qualitative research, this is not a general position, and most researchers feel that the issue of reliability is based in trustworthiness of the design process (Golafshani, 2003). For example trustworthiness of information can be achieved by collecting data through multiple key informants (Bonoma, 1985). In order to ensure that this research was conducted in a reliable manner, multiple informants were identified from the different banks and information collected from them. This reduces the risk of unbiased views being collected. Interviewees were also selected from different levels of responsibility (audit, forensic departments, risk management, fraud investigators) and seniority (managers, assistant managers, Heads of Departments) so as to collect and integrate a range of perceptions (Friedberg, 1993).

4.8.2 Validity

Validity in quantitative research is related to the concept of reliability. A construct that meets validity requirements must by default be reliable, but not vice versa. This means that a construct may be reliable but not valid (Netemeyer et al., 2003). The main issues in

quantitative validity in this research include construct validity and measurement validity. Construct validity refers to the ability of the identified items in the instrument to reflect the underlying constructs (Trochim & O'Donnelly, 2006). Construct validity was ensured in the pilot testing process, which included an analysis in order to examine whether the constructs being discussed in the research were those that were being perceived by the participants. This was also ensured in the qualitative research, by comparing the findings of the research to participant feedback in this area.

As with reliability, validity in qualitative research is a divergent concept from that of validity in quantitative research. Validity in qualitative research can encompass issues of construct validity, contingent validity, and analytical generalization, as well as rigor in the analysis process (Golafshani, 2003; Healy & Perry, 2000). These issues have been protected using careful analysis of the findings in order to ensure construct validity, including analysis by others (participants and other readers) as well as the researcher. The issue of contingent validity has been examined in the same way. However, the issue of analytical generalization has not been addressed, as this would not be easily determined from the structure of the survey.

4.8.3 Generalization of Findings

One of the weaknesses of the qualitative approach which was intended to be compensated for by the mixed methods research approach is the inability to generalize findings of the research (Creswell & Plano Clark, 2007). However, the quantitative research process has direct implications for generalization of findings. In this case, almost the entirety of the Kenyan banking industry was encompassed by the research, and so the application of these findings to the Kenyan context is appropriate. The quantitative results can be generalized with caution to banks in other countries in Africa with similar banking structures. The results may also be generalized with caution to international banks in Kenya as they were well represented in the survey.

4.8.4 Ethical considerations of the research

Ethical considerations were important in this study. Research ethics in this study has been guided by the Nottingham Trent University Graduate School code on research ethics. Throughout the duration of the research due care and attention was paid to protect all persons involved in giving information. The background and aims of the study were explained to the participants in a participants' information sheet attached to the questionnaire to ensure they understood the research. Issues of confidentiality, privacy, anonymity and informed consent were also outlined in the information sheet. Ensuring informed consent and giving a clear explanation about the nature of the research is useful in creating solid communication grounds from the start, can reduce attrition rates and increase the quality of data gathered. An assurance that the data collected would remain anonymous and all data will be based on aggregates was given to the research participants. The questionnaire did not ask for personal data such as name of the respondent or of the organisation, thus encouraging anonymity. Those being interviewed were also informed about the nature of the research in advance and they asked to sign a consent form before the start of each interview. Respondents being interviewed were given code numbers so that their identity was concealed to avoid traceability in the research report. All participants were informed that they had the right to opt out of the research at any time before the final publication of the thesis or to decline from divulging information they were not comfortable about. None of the participants have so far sought to withdraw their participation. However, during the interviews two interviewees declined to answer a question each stating that they were under a code of secrecy and could therefore not divulge certain information.

To enhance confidentiality and security interviews were recorded using a digital recorder and the data was later transferred to a secure laptop that only the researcher had access to. Any information that could be traced to or identified with a particular participant was removed from the transcripts and any subsequent write ups. Participant names and financial institution names were removed from the analysis process. Code numbers and pseudo-names were assigned to participants and banks so

that their identity was concealed to avoid traceability in the research report. Pseudo names were selected from Biblical characters. All data has been held securely in a locked cabinet and confidentiality of information divulged will be upheld. All audio files will be deleted or destroyed once they have been archived by the University in keeping with University rules.

4.9 Field Reflections

The research was carried out in the main capital city, Nairobi, where all banks have their headquarters. At first it was not easy to win the confidence of respondents as traditionally there has been a conservative culture where people are still very cautious about disclosing personal and organisational information to researchers. However, as the fieldwork progressed and the researcher got personally introduced, respondents gained more confidence and spoke freely. Younger managers were more open as most of them had experienced challenges of collecting information as postgraduate students and were therefore more sympathetic to the researchers' cause. Participants in the interviews all had a very positive attitude towards the research and expressed their desire to have a copy of the findings. Interestingly they did not mind being recorded and spoke freely in response to the interview questions. This shows a change in traditional culture where people that were once apprehensive about speaking out, even in terms not favourable towards their own organisation, have now embraced a new culture of openness and engagement with research. All the interviews were carried out at the convenience of the respondents in their offices or in a quiet room within the organisational building. The interviews lasted between 30 and 60 minutes. Due to the unavailability of time on the part of some participants at least three interviews were postponed and eventually cancelled.

However, it is worth pointing out that the response rate for the quantitative research was 75% (Sixty out of eighty possible respondents) and 85% for the qualitative study (Seventeen out of twenty possible respondents). This response rate makes this study as comparable as other research as it has adequately covered the banking industry; significantly it has captured the views of the leading banks that represent 70% of Kenya's banking market share.

4.10 Summary

This chapter has summarized the research process that was used in the study, in order to allow for critical examination of the findings, as well as replication of the research in other areas if possible. This has included discussion of the materials in terms of the qualitative and quantitative process, as well as the integration of the various findings. The research design and methods were then examined in light of the ways in which the research could be considered for generalization and replication. Not the entire results of the study would however be replicable due to the qualitative portion of the study, whose findings would be difficult to duplicate. This chapter has also discussed the various issues within the study, including reliability, validity, and ethics, and how these issues have affected the research. This chapter provides evidence that the research design was carefully constructed in accordance with the research philosophies in use, and that the findings of the research are founded in statistical and interpretive approaches. The study adopted a constructionism epistemology/ontology. Theoretical perspectives included both qualitative and quantitative approaches while research methods included a survey and semi-structured interviews. The next three chapters present the findings and outcomes of the study.

Chapter 5
Quantitative Study Results and Analysis

5.1 Introduction

This chapter discusses the results and analysis of the survey that was conducted. The main purpose of the survey was to collect information that would give a broad idea of the nature and characteristics of fraud in the Kenyan banking industry. The survey consisted of 29 quantitative questions, using a variety of question types including rankings, descriptive and interval-ratio questions. The questions were focused in four areas, including identification of the nature, trends, and characteristics of fraud, the experience of fraud in the organisation, fraud prevention techniques in use within the organisation, and information regarding the organisation and the role of the respondent in the organisation. This survey questionnaire is attached in Appendix 6. This survey was distributed to a sample of 60 individual respondents from organisations that met with the requirements of the study, the criteria of which are mentioned in the previous chapter. Following identification of hypotheses regarding the relationship between fraud and organisational characteristics (presented in Chapter 2), statistical analysis was performed using the statistical package SPSS. This analysis included descriptive statistics and inferential univariate and multivariate inferential statistical analysis, designed to both provide a hypothesis-testing approach and to identify any other relationships or patterns that could be seen within the data. An exploratory approach was used in order to identify any other potential relationships. Section 5.2 gives a review of the research questions the research is based on. Sections 5.3 and 5.4 present the analysis and discussion of the survey. Section 5.5 identifies the outcomes of the hypotheses testing procedure while Section 5.6 provides the findings in light of the research questions and the conceptual framework. Finally Section 5.7 summarizes the outcomes of the findings and analysis.

5.2 Review of the Research Questions

The following research questions were used in guiding the findings of the research. Of these research questions, Questions 1 and 2 are explored fully within this chapter, while

Question 3 is explored using both quantitative and qualitative findings (that is, split between Chapters 5 and 6). Research question 4 is discussed through some of the hypothesis outcomes and it is again discussed within Chapter 7.

1. What are the characteristics of fraud in the Kenyan banking industry?
2. What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?
3. How do banks approach fraud management?
4. Are there differences between the approaches to fraud management adopted by Kenyan and international banks?

5.3 Results and Analysis

The results of this study focused in three areas. First, in order to understand where the responses to the study have been derived from and the overall sample used for this study, a respondent study was built using the demographic and organisational information that was collected within the study. Second, descriptive statistics were provided that identified specific issues involved in the data set and described the distribution of variables. Third, statistical processes were used in order to identify relationships that were used to either prove or disprove the hypotheses that were stated above. The results of this research were then analysed in terms of the existing literature on fraud in the banking industry in order to determine where there were differences and similarities, as well as new insights that have emerged from the process of this research study.

5.3.1 Respondent Profile

This study was built on a sample of 60 respondents from 30 banking institutions selected from the population as described in the methodology chapter. A profile of the respondents has been built in order to determine the institutional and organisational context in which this research has taken place. The respondent profile included organisation-specific characteristics (including the description of the banking operation, the type of business organisation, the number of employees, and the turnover lost to fraud over the past year) as well as respondent-specific characteristics (including the position in

the organisation, the number of years in this organisation, and the number of years involved in the banking industry on the whole).

5.3.2 Organisational Characteristics

Table 5.1 provides a summary of categorical institutional characteristics, including the institution's general coverage, the corporate entity type based on respondents, and the number of employees within the organisation in Kenya.

Table 5.1 Descriptive characteristics of organisations

Description of the Institution (based on respondents)		
Institutional Description	Number of respondents	Per cent
Local Bank	19	31.7%
National Bank	8	13.3%
International Bank	21	35%
Regional Bank	12	20%
Total	60	100%
Corporate Structure Type of the Institution (based on respondents)		
Corporate Structure Type	Number of respondents	Per cent
Public Limited Company	32	53.3%
Private Limited Company	22	36.7%
Public Sector (Government)	6	10%
Total	60	100%
Number of Employees In the Institution (in Kenya)		
Number of Employees	Number of Respondents	Per cent
1 to 100	4	6.7%
101 to 500	23	38.3%
501 to 1,000	9	15%
1,001 to 10,000	24	40%
Total	60	100%

In terms of categorization, local banks are those whose operations were confined to Kenya; national banks are those in which the Government of Kenya has a substantial interest in by way of shareholding; regional banks are those that have operations in Kenya as well as in other African nations; and international banks are those whose operations cut across nations and continents of the world.

The most common types of banks based on respondents included local banks and international banks, with regional banks being a third common type. The most common corporate structure reflected was the Public Limited Company. Importantly, Table 5.2 (Cross-tabulation of organisation type and scope) shows that at least 75-76% of international and regional bank respondents surveyed were from Public limited institutions while most Local bank respondents (74%) were from Private limited companies; indicating that there was more public participation in international banks.

Table 5.2 Cross tabulation of Institutional description and corporate structure

Institutional Description	**n**	**Public Ltd (%)**	**Private Ltd (%)**	**Public Sector (%)**
Local Bank	19	26.3	73.7	0.0
National Bank	8	25.0	0.0	75.0
International Bank	21	76.2	23.8	0.0
Regional Bank	12	75.0	25.0	0.0
Total	60	53.3	36.7	10.0

The main non-categorical descriptive statistic used to build a profile for the banks was the amount of turnover lost to fraud each year, where turnover represents the annual revenue net of any sales returns. This was based on a percentage scale, with the minimum response indicating a loss of 0.01% and the maximum response indicating a loss of 5%. The mean for the full sample was 1.1757%, with a standard deviation of 0.84552. However, these figures varied somewhat from the mean when considering sub-samples based on the type of institution. The results of this analysis seem to indicate that fraud as

a percentage of annual turnover drops as the geographical spread of the banking institution gets wider. This was also analysed using the number of employees as the determining factor, in order to identify whether this was an issue unique to geographic coverage or if it was reflecting the size of the organisation. Table 5.3 identifies the means and standard deviations for each of the organisation type groups and employee size categories. These figures suggest a negative relationship between organisation size and percentage lost to fraud.

Table 5.3 Mean and standard deviation of fraud lost as a per cent of turnover annually, between organisational type categories and employee size categories

Organisation Type of the Institution	***Mean (%)***	***Standard Deviation***
Local Bank	1.4947	.29444
Regional Bank	1.0850	.20176
National Bank	1.0025	.18710
International Bank	1.0053	.07274
International Subsidiary	1.000	.50000
All Categories	1.1757	0.84552
Number of Employees	***Mean***	***Standard Deviation***
0 to 100	0.7750	.30380
101 to 500	1.0357	.13091
501 to 1,000	2.0667	.53774
1,001 to 10,000	1.0425	.07269

5.3.3 Respondent Characteristics

In addition to the institutional data observed above, there was also analysis of the data provided by the respondents to the study themselves. The responses for this study came from a wide variety of individuals within the banking institution, with varying degrees of responsibility within the organisation itself as well as a variety of levels of experience,

both within the organisation and outside it. Table 5.4 shows the job titles of respondents (which have been standardized but not collapsed).

Table 5.4 Role of the respondent in the organisation

Job Title	**Frequency**	**Percept**
Audit and Investigations/Internal Auditor	18	30.0%
Audit manager/Chief Internal Auditor	5	8.333%
Risk Manager	5	8.333%
Accountant	3	5.0%
Auditor (Internal)	3	5.0%
Fraud Investigation	3	5.0%
Fraud Prevention and Investigation/Operations	3	5.0%
Head of Security	2	3.3333%
Internal Investigations	2	3.3333%
Manager (Not further Specified)	2	3.3333%
Operations Manager	2	3.3333%
Security/Investigations Manager	2	3.3333%
Assurance Manager	1	1.6667%
Internal Control Monitor	1	1.6667%
Floor Services Manager	1	1.6667%
Forensic Manager/Forensic Auditor	1	1.6667%
Head of Accounting	1	1.6667%
Head of Finance	1	1.6667%
Heads Internal Control & Compliance Dept	1	1.6667%
Information System Auditor	1	1.6667%
Systems and Process Analyst	1	1.6667%
Validation Specialist	1	1.6667%
Total	60	100%

Respondent-specific questions included the number of years worked in the current institution, the number of years overall experience in the accounting or auditing field, and the role of the respondent in the organisation.

Table 5.4 shows a wide variety of respondents, and the majority of who fall into fraud prevention and detection, security and auditing job functions. The average overall accounting experience was 10.71 years while the average number of years the respondents had worked in the current institution was 6.9 years.

5.4 Descriptive Statistics

In order to understand the outcomes, it is important to understand the role that fraud has played within the organisations that have been examined. The descriptive statistics that have been conducted are based on four areas of discussion, including the overall view of fraud on the part of the respondent; experience of fraud (the types of fraud experienced, reasons for conducting such fraud, and who conducted the fraud, as well as the losses experienced and outcomes); the organisational climate responses to fraud; and the software integration responses to fraud.

Section 5.4.1 addressed Research Question 1 about the characteristics of fraud in the banking industry and the respondents view on this. Section 5.4.2 addressed the fraud experience of the respondent and captures Research Question 2 on the perceived characteristics of perpetrators as this section highlights who the perpetrator is, their motivation and rationalization. Section 5.4.3 considers the nature, kind and size of fraud addressing Research Question 1. Section 5.4.4 reviews Research Question 3 on how banks do fraud management.

5.4.1 Respondent's View of Fraud

This section deals with Research Question 1 which sought to understand the respondents' views on the characteristics of fraud in Kenya's banking industry. The first question was about how the respondents classify the fraud problem. Fifty four respondents (90%) indicated that it was a major problem as shown in Figure 5.1. This high percentage could

perhaps have been influenced by the nature of the respondents' job, which involves detecting and preventing fraud. These results are consistent with the general industry findings of the African Fraud and Misconduct survey (KPMG, 2005) that reported 72% of respondents indicated that fraud was a major problem.

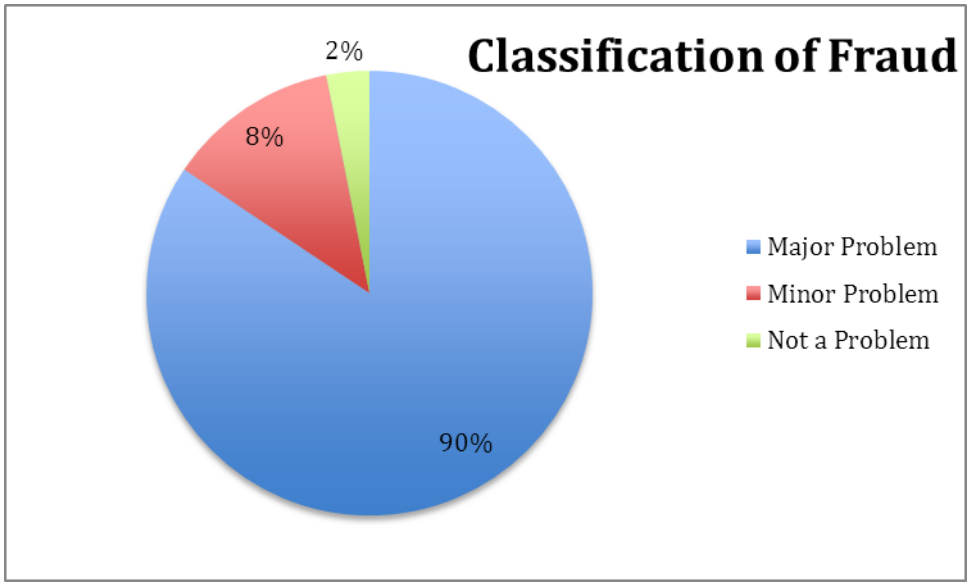


Figure 5.1 Classification of the fraud problem by respondents

The second question sought to find out how likely it was that fraud would be encountered in the financial sector. One respondent indicated that it was quite unlikely, while six (10%) respondents indicated that it was likely. Twelve respondents (20%) indicated that it was quite likely, while 41 respondents (68.3% of the sample) indicated that it was very likely. In total at least 98.3% respondents said that fraud is likely to occur over the next 5 years in the financial sector.

The third question focused on the direction of the trend in fraud. Three respondents indicated that it was decreasing, while seven indicated that it was remaining constant. Thirty-eight respondents indicated that it was increasing, while 12 respondents indicated that it was increasing rapidly (See Figure 5.2).

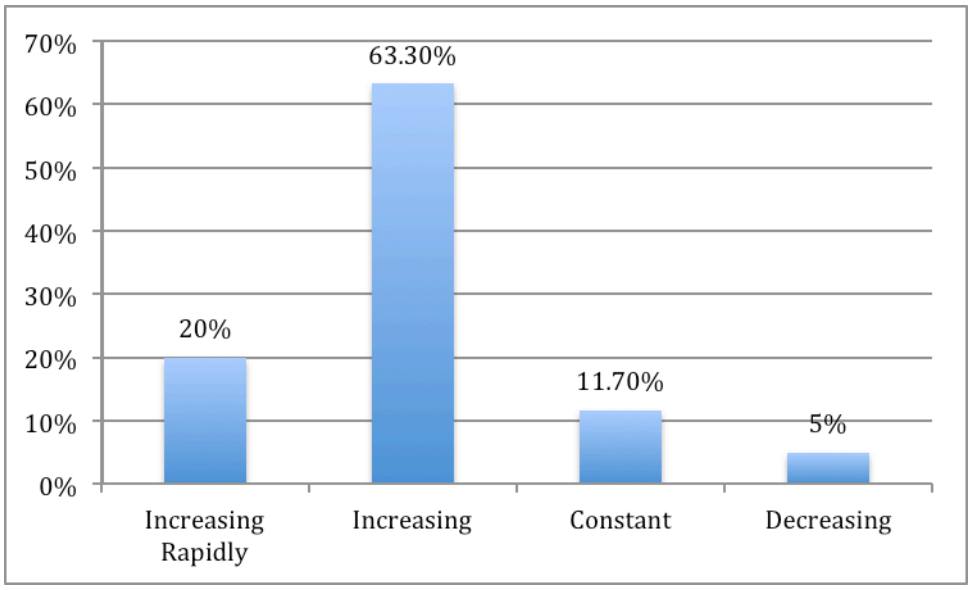


Figure 5.2 Trends in fraud

Table 5.5 cross-tabulates responses based on bank scope.

Table 5.5 Cross-tabulation: Fraud trends by bank scope

Bank Type	**n**	**Increasing (%)**	**Constant (%)**	**Decreasing (%)**
Local Banks	19	84.2	10.5	5.3
National Banks	8	75.0	25.0	0.0
International Banks	21	85.7	9.5	4.8
Regional	12	83.3	8.3	8.3

Again this finding is in tandem with findings of the African Fraud Survey (KPMG, 2005), which returned a similar opinion with 79% of the respondents expressing their opinion that the trend of fraud was on the increase.

Respondents were also asked to choose up to three reasons for the changes in the trend in banking fraud that they saw. These responses were not inherently ranked for importance. Table 5.6 demonstrates the reasons that were shown for the total fraud. This shows that

the most common reasons for changes in the trend of banking fraud include economic pressures, advanced computer technologies, and more sophisticated criminals.

Table 5.6 Reasons given for changes in bank trends

Reason	**Frequency (n=60x3=180)**	**Percept of total responses (173)**	**Percept of respondents indicating (60)**
Economic pressure	43	24.86	71.70
Advanced computer technologies	28	16.18	46.70
More sophisticated criminals	23	13.29	38.30
Ineffectiveness of justice systems	19	10.98	31.70
Changing society values	18	10.40	30.00
Inadequate fraud training	16	9.25	26.70
Poor management practices	11	6.36	18.30
Social-cultural factors	6	3.47	10.00
Poor ethical practices	6	3.47	10.00
Political factors	3	1.73	5.00

These figures did not show significant differences based on the size and scope of the banking operation. Although there were some percentage differences, this was due to dramatic difference in the size of the categories, as well as one local bank respondent with an outlying view of the severity of the fraud problem. Full cross-tabulation tables for this investigation are available in the Appendix IA.

5.4.2 The Experience of Fraud

The second group of questions focused on the experience of fraud over the past year, identifying perpetrator characteristics, losses, and reasons given for the fraud. This is intended to characterize the scope and scale of fraud as experienced by respondents in their organisations, and this is also analysed depending on the organisation type in order to determine if there are any significant differences between institutions based on scope of the institution. This Section addresses Research Question 2.

5.4.2.1 Who Perpetrates Fraud?

Research question 2 read, "What are the perceived characteristics of those that perpetrate fraud?" The quantitative insight into this question is demonstrated within this section. One group of questions asked in this survey focuses on the perpetrator characteristics, including the position or role of each perpetrator, their age, gender, and other characteristics. This information was compiled from the views expressed by those employed to counteract fraud in the organisation and not from the fraudsters involved in the committing the fraud. Information regarding educational level, though important in other studies (Sutherland, 1949; Krambia, 2004; Wheeler, Weisburd and Bode, 1988) was not routinely available and so was excluded; The minimum educational level of internal perpetrators can be inferred as Kenyan banks require a secondary school education for positions such as cashiers, tellers etc.

The most common organisation was collusion between internal and external perpetrators (N = 42), and the second most common was collusion between internal perpetrators (N = 8).

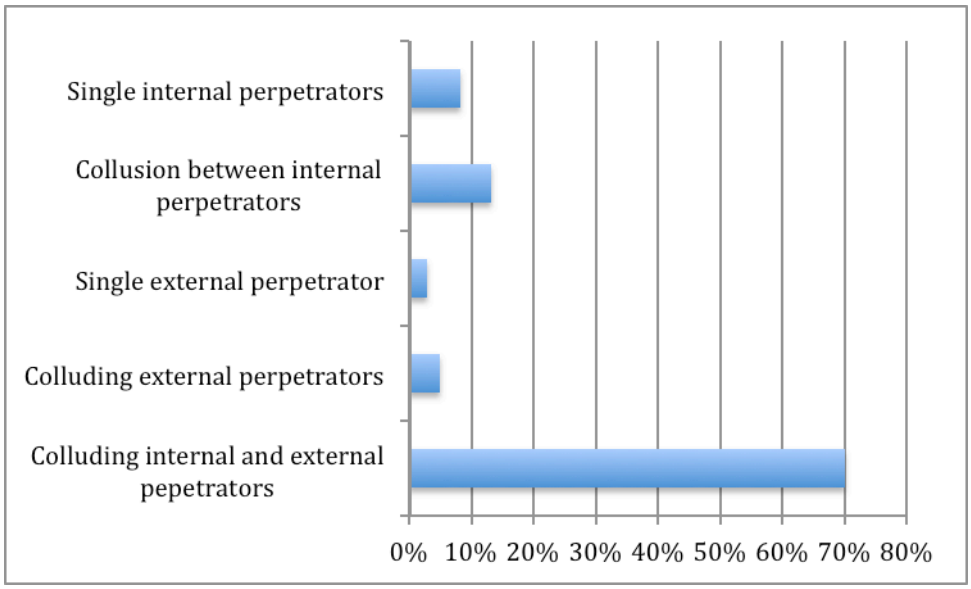


Figure 5.3 Fraud perpetrators by type of conspiracy

These findings agree with the KMPG (2005) report that revealed that over 75% of frauds are perpetrated by employees in Kenyan organisations and that collusion is the number

one form of fraud in the organisations surveyed. If collusion between external perpetrators is included then the overall rate of collusion moves up to 88%, leaving single perpetrators in only 12% of cases. This raises an important question as to whether earlier criminology theories that emphasized the individual characteristics and circumstances of fraudsters may have over-simplified real situations.

The second issue that emerged was the relative positions of internal and external first and second parties. Table 5.7 demonstrates the positions or roles of the parties that engaged in the fraud. This shows that a total of 87 internal perpetrators and 78 external perpetrators were involved in the overall level of fraud.

Table 5.7 Role and position of perpetrators

Role and Position of Perpetrators			
Internal Roles	First Party	Second Party	Total
An Executive (Director/Officer)	2	1	3
A junior manager	5	9	14
A middle manager	9	3	12
A senior manager	6	2	8
A junior non-managerial employee	18	6	24
A middle non-managerial employee	8	4	12
A supervisor	6	7	13
An Owner	1	0	1
Total	**55**	**32**	**87**
External Roles			
A Customer	20	7	27
A competitor	1	1	2
A supplier	3	4	7
A Contractor	2	0	2
A former Employee	6	10	16
An organised Criminal	13	2	15
A company agent	3	2	5
A Friend	2	0	2
Other	0	2	2
Total	**50**	**28**	**78**

Collusion between internal perpetrators mainly involved junior non-managerial employees as the internal first party (main perpetrator) and either a Supervisor or a junior manager as the internal second party (the accomplice). Early studies in white-collar crime showed that the position held by the perpetrator in the victim organisation played a role in the kind of fraud committed (Cressey, 1973). This is because the perpetrator will possess technical knowledge by virtue of the fiduciary duties and position of trust that they occupy that enables them to perpetrator the fraud. This finding therefore supports the work of Cressey (1973). Friedrichs (2004) and Vaughan (2001) have argued that employees in junior positions can only commit certain types of fraud as their opportunities would be limited by their position while those in higher managerial or executive positions may have access to more opportunities based on the greater degree of trust vested in their position.

The main external parties involved in the fraud were bank customers and organised criminals as the external first parties and former employees as the external second parties. The African Fraud Survey (KPMG, 2005) supports this outcome as it also indicated that customers were the next highest group of perpetrators after employees making them the top external party to fraudulent activities.

The survey also collected information on reported age and gender of the fraudsters. Table 5.8 shows the age and gender of primary and secondary internal perpetrators in order to allow for comparison. (This information was not reported for all parties). The majority of both internal and external perpetrators are between 31 and 40 and male. This is approximately consistent with findings previous research, including Benson and Moore (1992); Holtfreter (2005); Krambia (2004); Wheeler et al. (1988). This did not quite agree with previous studies carried out by Wheeler et al (1988) who found that the typical offender was white male aged forty on average. However, the study by Wheeler et al (1988) was carried out in America. Kenya is a relatively ‘younger’ society than America and has a different cultural setting. One could therefore argue that the context of Wheeler et al (1988) study varies from that of this research.

Table 5.8: Age and Gender of Parties Involved in Fraud

Age of Parties Involved in Fraud			
Internal	1st Party	2nd Party	Total
Below 30yrs	19	9	28
31-40yrs	28	21	49
41-50yrs	6	2	8
Over 50yrs	1	1	2
External	1st Party	2nd Party	Total
Below 30yrs	7	2	9
31-40yrs	30	22	52
41-50yrs	9	1	10
Over 50yrs	1	1	2
Gender of Parties Involve in Fraud			
Internal	1st Party	2nd Party	Total
Male	43	23	66
Female	12	11	23
External			
Male	44	22	66
Female	5	5	10

There are relatively few studies on gender and fraud either in Kenya or generally (Daly, 1989; Heimer, 2000, as cited in Holtfreter, 2005; Steffensmeier, 1993). Press reports also indicate that there is little known about the gender breakdown of fraud in Kenya (Okwembah, 2010). This research shows that women are a minority participant in fraud, which is inconsistent with the findings on fraud in previous research (Holtfreter, 2005). This could be due to relatively low status of women in Kenyan banks, whose roles as

receptionists or tellers do not offer sufficient basis for collusion (Daly, 1989; Friedrichs, 2004; Vaughan, 2001). There were no significant differences found in distribution between the various types of banks surveyed in the position, gender, or age of internal or external fraud perpetrators. Full cross-tabulations are available in the Appendix (Statistical Outcomes/Cross Tabulations).

5.4.2.2 Motivations and Rationalizations for Fraud

In addition to the types of fraud and the frequency of various types of fraud, this research also examined the identified motivations (pressures) and rationalizations (justifications) for the fraudulent activities involved. It should be noted that as this information came from the bank employees rather than the fraud perpetrators, this is a third-party assessment for the reasons involved in the fraudulent activity. Table 5.9 shows the relative frequency of various motivations for the fraud. These figures demonstrate that opportunity, lifestyle habits, personal financial pressure and greed were the most frequent motivating factors in the responses. These findings generally support findings of a KPMG (2007) study.

Table 5.9: Motivating factors for fraud

Motivating Factor	**Frequency (n=60)**	**Percept (%)**
Opportunity	38	63.3
Lifestyle habits	28	46.7
Personal financial pressure	24	40.0
Greed	21	35.0
Others	5	8.3
Substance Abuse	3	5.0
Gambling	2	3.3
Corporate financial pressure	2	3.3

Results indicated that most perpetrators commit fraud from opportunity rather than need supports the predator concept (Kranacher et al., 2011). Under this model, the fraudster seeks out opportunities to commit fraud immediately, and do not require rationalization or pressure, but only opportunity (Dorminey et al., 2010). This is inconsistent with the fraud triangle theory, in which an individual gradually gives in (Kranacher et al., 2011). However, this is only indicative and since responses were not reported by fraudsters, this could be skewed. The research findings also confirmed that non-shareable problems,

including financial pressures, living beyond one's means, social pressures, and greed as advanced by Cressey (1973) were motivators of fraud.

Respondents were also asked about reasons given by perpetrators, in order to determine rationalizations used by fraudsters during the fraud process (Cressey, 1973). Table 5.10 reflects the most common reasons reported which included getting rich quick, family pressure and the fact that others get away with it. As with the motivation of fraud discussed above the same status gaining and societal justifications have been advanced. However employer-employee relations (such as being under-paid and seeking revenge on the organization) did not seem to feature highly as justifications for fraud which could be an indicator that internal perpetrators were generally satisfied with their job or as predators would see the job as an opportunity to commit fraud. It is significant to note that about 20% of respondents were not sure as to why fraud was committed.

Table 5.10: Justification of fraud given by perpetrators

Reasons	**Frequency (n=60)**	**Percept (%)**
To get rich quick	23	38.3
Others are getting away with fraud	14	23.3
Had family pressure	14	23.3
Don't know	13	21.7
Influenced/forced by others	9	15.0
Was just borrowing hoping to repay	9	15.0
Underpaid	8	13.3
Others	6	10.0
Was seeking revenge on the organisation	3	5.0
Everyone else around them were fraudulent	2	3.3
The amount of money taken was not too large a sum	2	3.3

5.4.2.3 Reasons why fraud occurred (Opportunities)

One of the questions focused on the respondent identifying the organizational reasons as to why the fraud occurred. This question essentially sought to know the reasons why the fraud was successful and what opportunities in the organization had led to the fraud occurring. Each respondent was to identify up to a maximum of 3 reasons. It should be noted that not all respondents identified 3 reasons as it was possible to have only one reason or opportunity. Table 5.11 indicates the reasons why fraud occurred.

Table 5.11 Institutional or organizational reasons why fraud occurred

	Frequency				
Reason	Primary Reason	Secondary Reason	Tertiary Reason	Total (n=60)	Percentage
Poor internal controls	27	9	2	38	63.33
Overrides of internal controls by management	7	11	4	22	36.67
Poor screening procedures on hiring	18	-	-	18	30
Poor organizational culture	2	8	4	14	23.33
Use of new technology and systems	-	2	10	12	20
Poor record keeping, lack of documentation	2	4	4	10	16.67
Lack of fraud training	1	4	3	8	13.33
Other	1	4	2	7	11.67
Poor inventory control	1	2	2	5	8.33
Failure to punish offenders	-	1	3	4	6.67
Lack of ethical culture	2	-	-	2	3.33

Poor internal controls and overrides of internal controls by management were cited as the main reasons why fraud occurred. Internal controls importantly play a vital role in the prevention, detection and deterrence of fraud (Porter, 2003). Strong internal controls can discourage attempts to defraud an organization while poor internal controls invite fraud

into the firm. However internal controls can become ineffective in the face of collusion especially where management or employees are involved. Overrides by the management weaken internal controls rendering them ineffective and opening a door to fraud. The results of this study support earlier studies carried out by the Association of Certified Fraud Examiners (ACFE, 2008) which found that the lack of internal controls was the most commonly cited weakness with overrides by management being ranked the number three weakness

Poor screening procedures on recruitment also provided a significant opportunity in the commission of fraud. The recruitment and selection process is an important aspect of human resource strategies that can help to reduce the risk of fraud occurrence. The finding on poor screening procedures in Kenyan banks is consistent with findings of the study carried out by Meyer et al (2011) which indicated that firms in South Africa often have poor recruitment practices mainly arising from structural problems that create an inability to depend on previous employers for references before recruiting an employee. As observed from banks in Tanzania (Newenham-Kawindi, 2011), banks in Kenya need to monitor and remain in control of the recruitment process even when activities are outsourced. Recruiting the right people who possess the right skills while developing and training bank staff to increase human resource capacity is a strategy that can be adopted by the banks in Kenya (Kamoche, 2011; Oshikoya, 2010)

5.4.3 Profile of the Fraud

In addition to the perpetrators, the research collected data on the type of fraud. This included the type of the fraud, the nature of the fraud, any ancillary fraud conducted during the commission of the main fraud, the motivation for the fraud, the reasons given by the perpetrators where known, the overall level of loss due to the fraud, actions taken by the bank, outcomes of these actions, and any financial recovery the bank received. This discussion reflects on Research Question 1, “What are the characteristics of fraud in the Kenyan banking industry?”

5.4.3.1 Types of Fraud

The first question was what type of fraud was observed. Figure 5.4 shows the relative popularity of various types of negotiable instruments and assets that were the target of frauds.

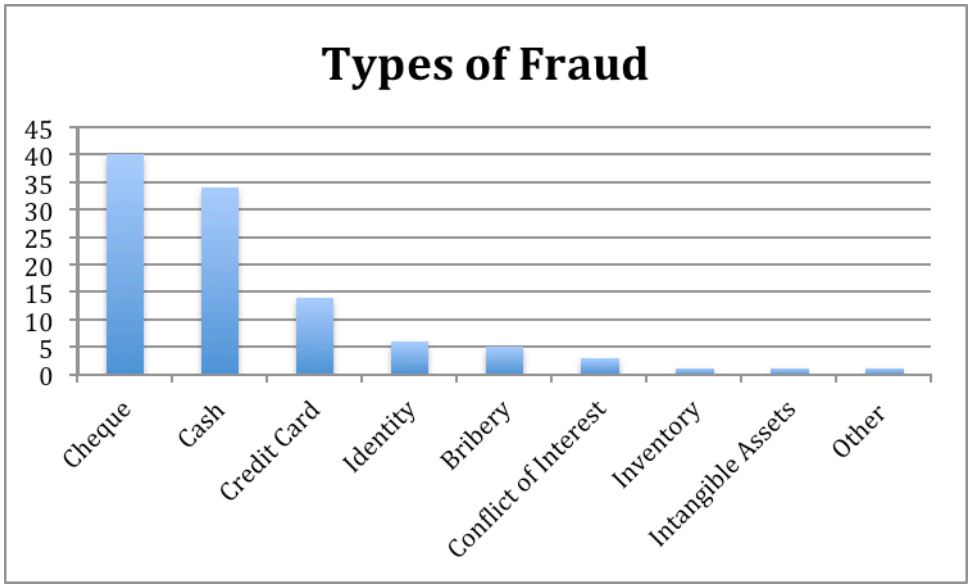


Figure 5.4 Types of fraud

This shows that the most popular types fraud based on frequency numbers were cheques (n=60; 66.66% of respondents), cash theft (58.33% of respondents), and credit cards (23.33% of respondents) with identity theft and bribery or kickbacks being secondary. This finding is consistent with reports appearing both in a national newspaper (Okwemba, 2010) and on the local television news (KTN, 2010) revealing that cheque fraud was the most common type of fraud suffered by the banking industry in the first quarter of 2010.

Table 5.12 demonstrates the frequency of the various types of fraud that were involved. The main types of fraud were theft and diversion (theft refers to the taking of money while diversion and misappropriation refer to assignment of funds to other areas). Conversion frauds are those that are used to conduct other frauds. Abuse and misuse frauds refer to frauds associated with violation of bank policies for personal gain, while infringement was primarily inappropriate seizure of private customer information.

Table 5.12 Nature of the fraud

Nature of fraud	Frequency (n=60)	Percept (%)
Theft	44	73.3
Diversion/Misappropriation	31	51.7
Conversion	16	26.7
Abuse/Misuse	10	16.7
Infringement	4	6.7
Others	4	6.7

Figure 5.5 compares nature of theft by type of institution, showing that theft was highest ranked in all cases.

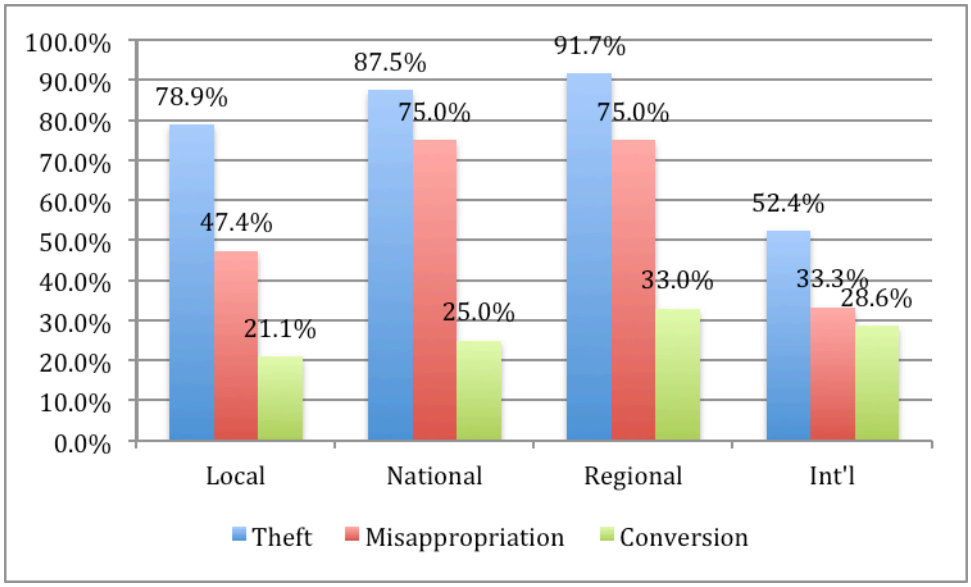


Figure 5.5 Top three fraud types by bank scope

A number of the frauds involved secondary or ancillary frauds that were used in order to support or hide the main fraud approach. Table 5.13 shows the most common ancillary frauds that were reported. Once again, the vast majority of ancillary fraudulent activity was concentrated in three areas, transfer of funds, computer fraud and identity theft or

fraud. These findings are consistent with the Central Bank of Kenya's first and second quarter 2010 reports.

Table 5.13: Frequencies of various ancillary frauds

Type of fraud	**Frequency (n=60)**	**Percept (%)**
Transfer of funds	39	66.1
Identity fraud	32	54.2
The use of computers (computer fraud)	22	37.3
Falsified accounts and financial statements	14	23.7
False invoicing	5	8.5
Fraudulent expense claim	3	5.1

5.4.3.2 Monetary Losses

Overall loss from fraud was estimated as both a percentage of the organisation's revenues (revenue) and as a fixed figure (presented in Kenyan shillings). Figure 5.6 demonstrates the overall monetary loss for a typical year demonstrated categorically as a percentage of the organisation's revenues. A majority of the organizations reported a monetary loss of less than one per cent of the revenue, although a small number of organisations had a loss of up to 5%.

Some of the respondents provided more exact estimates of the overall loss to the organisation. The mean loss to the organisation for those that provided this information in Kenyan Shillings (KES) (N = 25) was KES 21,641,000 (approximately USD $277,000 or €224,000 as of May 14, 2010), with a median loss of KES 5,000,000 and a standard deviation of 55,740,700 KES (€577,000 or US$ 713,000). This dramatic right-skewed distribution can be attributed to a single outlying instance of very high value fraud, where a total of 271,000,000 KES (US$ 3,466,000 or €2,804,000) was lost. The minimum fraud that was disclosed was KES 118,000 (approximately €1,221 or US$ 1,509). This

demonstrates a wide variance in the loss of funds as an overall total from the banks. This data is however restricted to known or detected fraud that has been reported.

A number of banks also provided information regarding the loss to the organisation in terms of the loss of a single fraud as a percentage of annual revenue. The mean overall loss reported as a percentage of revenues (N = 27) was 1.57%, with a median 1% and a standard deviation of 2.93%. The minimum was 0.10%, with the maximum being 16%.

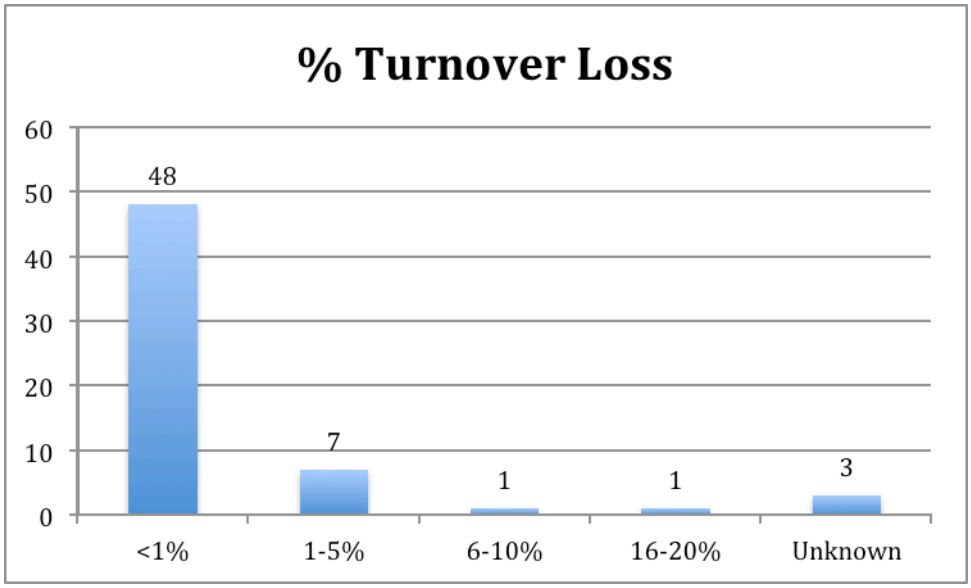


Figure 5.6 Estimated overall loss as a per cent of projected annual revenues

These estimated losses are only indicative of the potential problem fraud is within the banking industry. The only similar studies relate to the ACFE (2008) report where it was reported that the average loss for organisations in the USA is 7%. However, this considers more industries than just the banking industry considered under the current study. Closer to home the African fraud survey (KPMG, 2005) categorised 17% of the loss as ranging over USD$170,000 for all the industries surveyed in that study. A direct comparison cannot be made but it shows that fraud losses continue to be incurred and are likely to increase further given the general opinion about fraud.

5.4.4 Organisational Responses to Fraud

Research question 3 asks how banks approach fraud management. This question is addressed in two ways, including discussion of the detection and investigation of specific frauds as well as organizational and technological approaches to prevention and detection.

5.4.4.1 Detection and Investigation of Fraud

Fraud was detected in a variety of ways, with some organisations using more than one method of detection. Figure 5.7 identifies the main type and frequency of the different ways in which fraud could be detected.

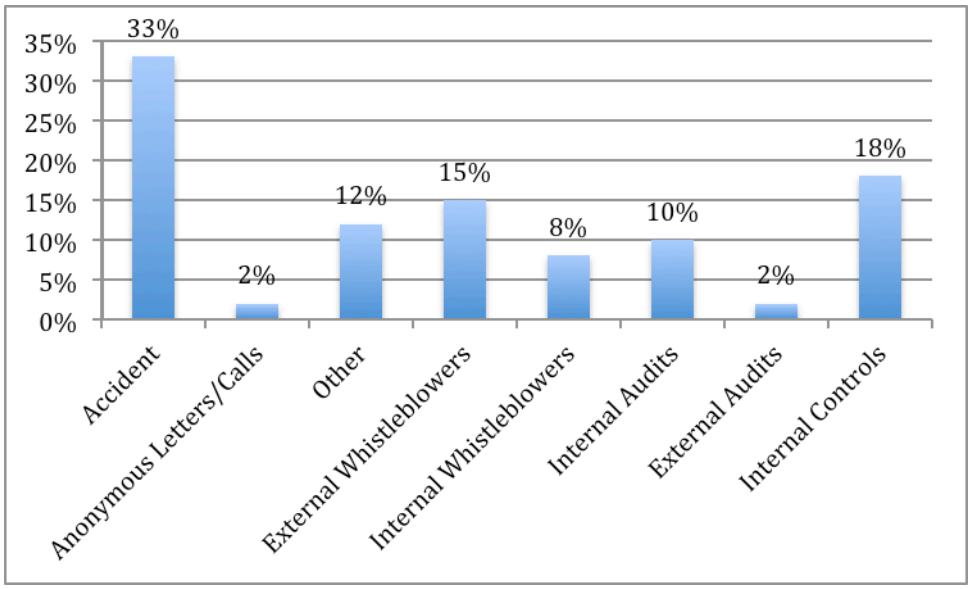


Figure 5.7 Ways in which fraud was detected

The data shows that one- third of the incidents were discovered by accident. The use of external auditing was one of the least useful methods of detection of fraud, with the same number of frauds being detected by anonymous letters or calls regarding the occurrence. In contrast, whistle-blowers (23.3%), and accountholder and customer complaints (12%) were popularly resorted to as methods of discovering fraud. As the use of other methods of fraud detection like whistle-blowing and internals controls increases then the likelihood of fraud being detected by accident should be reduced (ACFE, 2008). This is inconsistent with previous studies showing that rated internal controls as being the most commonly used detection method followed by whistle-blowing and then by accidental

discovery (KPMG, 2005). The difference in results from all these studies implies that there is no one universal or static method for fraud detection, making fraud detection and fraud detection methods fluid subjects.

Organisations varied widely in who investigated the fraud, and some organisations used multiple investigators in order to investigate the crime. The most common bodies involved in the investigation (See Table 5.14) included internal investigation by a security department, investigation by a law enforcement body, and review of a case by internal audit committee.

Table 5.14: Investigating parties in reported frauds

Investigator Type	**Frequency (n=60)**	**Percept (%)**
Internal Investigation by Security Department	39	65.0
Law enforcement body	28	46.7
Case reviewed by internal audit committee	17	28.3
Risk managers	8	13.3
Forensic Accountants	6	10.0
Private Investigators	5	8.3
Internal Investigation by Finance Department	4	6.7
Government regulatory body	2	3.3
External auditors	1	1.7
Fraud specialists	1	1.7
Operations team	1	1.7

There appears to be a preference by banks in Kenya to attempt investigating fraud cases internally by mainly resolving them through the Security Departments or the Audit Committees. This could be an image saving approach as the banks do not have to expose their fraud problems to external parties and risk damaging their reputation. However,

there are also a considerable percentage of respondents that indicated that a law enforcement body was involved in fraud investigation. This could be an indicator that almost half the fraud cases are reported to a law enforcing body.

5.4.4.2 Actions and Outcomes

Following the discovery of the theft, there were a number of actions the organisations could take, including civil or criminal prosecution, negotiated settlement, dismissal, disciplinary hearings, or others. Table 5.15 identifies the main responses that were observed in the data set regarding first and second internal and external parties to the fraud and it shows that the most frequent action in the case of internal parties was immediate dismissal, followed by criminal prosecution.

Table 5.15 Actions taken against the parties involved in the fraud on discovery

Internal Parties	1st Party (%)	2nd Party (%)
Immediate dismissal	78.2%	68.8%
Disciplinary action other than dismissal	7.3%	12.5%
Allowed employees to resign	10.9%	15.6%
Criminal prosecution	30.9%	28.1%
Civil prosecution for recovery	10.9%	6.3%
Negotiated settlement	1.8%	
Other action	1.8%	
External Parties		
Civil prosecution for recovery	23.3%	28.6%
Criminal prosecution	80.0%	61.9%
Negotiated settlement	3.3%	4.8%
Took no action	50.0%	33.3%

The most common response for external parties was criminal prosecution, followed by civil prosecution. This does indicate that in the case of external parties almost all of the external parties faced criminal or civil prosecution. Where action was taken 80% (i.e. 80% of the fraud cases on external 1st parties were referred for criminal prosecution and about 62% of fraud cases on external 2nd parties were referred to the courts for civil prosecution. However, rates of legal redress were somewhat lower for primary and secondary internal parties compared to external parties. The rates of negotiated or arbitrated cases were very low.

The discussion under hypothesis 2b (Section 5.5.2) analyses if this difference is statistically significant. There were a high percentage of cases where no action was taken on external parties with 50% of external primary parties and almost 77% of external secondary parties walking away scot free with fraudulent acts. As discussed further in Chapters 6 (Section 6.4) legal issues surrounding the drawn out period of time it takes to secure a conviction, high acquittal rates, problems of police slackness and frequent transfers, unskilled fraud prosecutors, inadequate legislature to prosecute criminals, weak legal enforcement and poor industry co-operation among the banks are among some of the reasons why banks opt not to follow up on fraud cases. Sometimes the cost involved in pursuing a fraud case in terms of the legal fees and time spent far outweighs the benefit that the organisation will receive from the case.

Respondents were also asked what the outcome of their actions against fraud perpetrators was (in the case of civil or criminal prosecution). Table 5.16 summarizes the outcome of actions against internal and external parties. (Percentages have been calculated on total number of cases reported, in order to ease difficulties with the number of parties involved).

Table 5.16 shows that the chance of securing a conviction is more likely when an external party is concerned. However, it is also true to observe that a high percentage of cases were on-going and still before the courts.

Table 5.16 Outcome or status of criminal and civil courses

	Internal 1st party (N = 29)	Internal 2nd Party (N = 15)	External 1st Party (N = 32)	External 2nd Party (N = 19)
Acquittal	20.7%	6.7%	12.5%	10.5%
Conviction	34.5%	20.0%	43.8%	36.8%
Negotiated Settlement	10.3%	20.0%	12.5%	10.5%
On-going case	34.5%	33.3%	31.3%	42.1%

The final outcome-based variable was the extent of financial recovery the organisations had realized. Figures in Table 5.17 show that, regardless of the category of perpetrator in the fraud, realization of financial recovery is very rare, but there are somewhat higher recoveries from internal fraud perpetrators than from external fraud perpetrators.

Table 5.17 Extent of financial recovery from fraud perpetrators

Extent of Recovery	Internal 1st Party (n=52) (%)	Internal 2nd Party (n=30) (%)	External 1st Party (n=41) (%)	External 2nd Party (n=26) (%)
None (0%)	71.2	66.7	82.9	84.6
Partial	15.4	23.3	9.8	11.5
Full (100%)	13.5	10.0	7.3	3.8

5.4.4.3 Fraud Prevention measures

The importance and use of fraud prevention measures were examined using ranked items that asked how useful each of the potential organisational responses was, with 1 indicating most important and 5 indicating least important for a maximum of five responses. Table 5.18 describes the mean, median, and standard deviation of each of these measures, as well as the number of responses ranked against each measure.

Table 5.18 Ranked importance of organisational measures

Organisational Approach	Mean	Median	Std. Dev.	n
Improvement or review of internal controls	1.53	1	0.979	55
Training employees on fraud prevention	2.75	3	1.184	44
Establishing fraud prevention policies	2.78	3	1.205	37
Ethical code of conduct	3.32	4	1.282	25
Implementing a fraud hotline	3.61	4	0.891	23
Screening/reference checks	3.19	3	1.327	21
Staff rotation policy	4.19	4	0.834	16
Security department	3.55	4	1.440	11
Automated fraud prevention	4	5	1.265	11
Close supervision	4.1	4.5	1.101	10
Spot checking	4.1	4	0.994	10
Limiting opportunities	3.29	3	1.704	7
Ethics training	3.83	4	0.983	6
Fraud auditing	4.33	4.5	0.816	6
High deterrence measures	3.2	3	1.483	5
Use of forensic accountants	2.25	2	0.500	4
Establishing a fraud budget	2.75	2.5	2.062	4
Others	4	5	1.732	3
Surveillance of electronic correspondence	2	2	0.000	1
Inventory observation	5	5	0.000	1

Table 5.18 demonstrates that there are some inconsistencies between the relative importance of measures and the number of banks using these measures. The five most commonly used measures included improvement or review of internal controls (N = 55), the use of fraud prevention training (N = 44), the use of fraud prevention policies (N = 37), the use of an ethical conduct code (N = 25) and the use of a fraud hotline (N = 23).

However, independent t-testing for differences in means indicates that the mean importance ranking for ethical code of conduct and fraud prevention are not consistent with the frequency of the fraud prevention measures. This data is available in the Appendix (T-Tests).

The responses that were ranked highly, but only by a small group, may be interpreted as being highly effective or important responses in organizational contexts that require them, but that are not routinely used. One such example is forensic accountants, which are ranked number 3 in mean importance among users despite the relative rarity of their use. This indicates that banks that *do* use forensic accountants consider them to be very important, but that their actual use is rare.

The research has upheld the general perceived effectiveness of the internal control and audit and its widespread use within the organisation, as identified by a number of other researchers as being an important element in the prevention and detection of fraud (Bostan, 2010; Greenlee et al., 2007; Hillison et al., 1999; Moeller, 2004; Adams, 1994). The use of internal auditors has been shown to be consistent with findings by other researchers. This indicates that, despite any potential difference between the African and Anglo-American business models, internal controls still have the potential to be effective in cases where they have been implemented appropriately, as consistent with previous research in this area (Black & Geletkanycz, 2006; Palmer et al. 2008).

5.4.4.4 Software Usage

In addition to organisational responses, the respondents were asked what kind of software they used in their respective banks and how effective it was. The types of software security protocols that were examined included password protections, antivirus software, continuous auditing software, firewalls, discovery sampling, ratio analysis, digital analysis, data mining, and filtering software. All of the organisations reported some use of software security protocols, with the minimum number of protocols in use being 2 and the maximum being 9. Overall, the sample showed a mean of 5 types of software-based security protocols, with a standard deviation of 1.896.

Table 5.19 shows the use and efficacy of each type of product. Antivirus software and password protection were used almost ubiquitously within the organisations. The use of anti-virus software is important in providing protection to the business websites against attacks from computer spyware and malware that can mimic the genuine business website leading to customers being defrauded through their account details being captured by counterfeit websites. Continuous auditing is being used by more than three quarters of the sample.

The most effective software that was identified was digital analysis (100% rankings in highly effective and effective) along with data mining. However, though effective, few banks were making use of them. Of those using discovery sampling a number of them were not sure about its effectiveness.

Table 5.19 Software use and perceptions of effectiveness

Software Type	Use		Effectiveness			
	Yes	No	Highly Effective	Effective	Ineffective	Unknown
Antivirus Software	59	1	20 (34.5%)	34 (57.6%)	4 (6.8%	1 (1.7%)
Password Protection	58	2	23 (39.7%)	31 (53.4%)	4 (6.9%)	
Continuous Auditing	46	4	12 (26.1%)	31 (67.4%)	3 (6.5%)	
Filtering	38	22	14 (36.8%)	15 (39.5%)	7 (18.4%	2 (5.3%)
Firewalls	25	35	11 (44%)	12 (48%)	1 (4%)	1 (4%)
Discovery Sampling	24	36	6 (25%)	13 (54.2%)	1 (4.2%)	4 (16.7%)
Data Mining	22	38	16 (72.7%)	4 (18.2%)	2 (9.1%)	
Ratio Analysis	18	42	5 (27.8%)	10 (55.6%)	3 (16.7%)	
Digital Analysis	10	50	8 (80%)	2 (20%)		

Digital analysis, discovery sampling and data mining are of particular importance given that these are the most technologically advanced methods and the ones with the most importance in terms of hidden fraud discovery. These findings concerning software effectiveness are consistent with results of Bierstaker et al. (2006) who found that even though data mining, digital analysis and discovery sampling were not used by majority of organisations they were ranked by participants of the study as being the most effective methods. Just like Bierstaker et al. (2006) this study has found that the more popular software approaches used for fraud prevention (i.e. firewalls, virus protection, password protection) are not as effective.

The role of information security has been promoted as one of the determining factors in the effective prevention of internal and external fraud (Baloyi, 2005; Bielski, 2004; Bierstaker et al., 2006; Bolton & Hand, 2002; Haugen & Selin, 1999; Tipton & Krause, 2006). The overall effectiveness as perceived by the respondents of software approaches to fraud detection and prevention was positive, with most methods being considered to be very effective or effective. However, this did not appear to translate into a direct reduction in the degree of fraud experienced by the banks. Some of the possibilities for this seeming disconnect in the relationship between bank losses and software effectiveness are either that the assessment of software effectiveness is overstated, or that there is a threshold of fraud below which the use of software cannot be overly effective. This is likely to occur when insiders have a heavy involvement in the practice of fraud, as insiders will understand the software detection systems in place and will understand what types of fraud are most likely to go unnoticed. Given this, it is likely that, given the relative uniformity in application of software across banks, the role of software in reducing frauds is consistent across banks and other variances are due to issues like insider access. However it is also possible that fraudsters behave like a ‘moving target’ in that as information technology (IT) based measures respond to their innovations fraudsters may shift their attention to other system weaknesses.

5.4.4.5 Organisational Response Discussion

The role of organisational culture in fraud reduction is supported by a large number of previous studies (Mawhinney, 2009; May, 2003; Moorthy et al., 2009; Porter, 2003; Stringer & Carey, 2006; Tipton & Krause, 2006; Wells, 2004). The majority of studies that have been performed on fraud in the banking system, as well as organisational fraud generally have been conducted in an Anglo-American business environment (in the United States or Great Britain, or in Commonwealth countries). However, there are significant differences in the emergent African business model (Sardanis, 2007). Some changes, such as ethics training or anonymous hotline establishment, have been slow in gaining acceptance in the business environment where this research was conducted. The use of organisational change management practices can promote positive change within the organisation, and may be useful in some of the banks in order to improve organisational practice toward fraud prevention (Palmer et al., 2008).

5.4.5 Descriptive Summary

The results of the descriptive testing can be summarized as follows. Most respondents felt that fraud was a large and growing problem. Most frauds were collusion between internal and external perpetrators, including junior managers and non-managerial employees, customers, and former employees, male and aged 31-40. Motivations included opportunity and lifestyle issues; rationalizations included getting rich, family pressure, and others engaging in fraud while organizational fraud opportunities mainly presented themselves through poor internal controls, over-rides of internal controls and poor screening procedures on recruitment. Most fraud targeted cheques, cash, and credit cards, with fraud involving theft and diversion. Tools were mostly computer-based; identify fraud and theft, and falsification of accounts.

Most frauds were detected through accident, internal controls, and external whistle-blowers. Investigation was commonly performed by internal security departments and law enforcement bodies. Most institutions lost below 1% of annual turnovers, with more precise figures indicating loss of KES21.6 million or 1.57% of revenues. Responses involved dismissal and prosecution as well as civil prosecution. Conviction rates ranged

from 10.5% to 43.8%. Financial recovery was rare. Organisational responses included review of internal controls and training employees. Software used included antivirus software, password protection, and continuous auditing. However, the least used approaches, data mining and digital analysis, were also deemed to be the most effective. The low uptake of these highly effective methods could be due to the cost involved in implementing them.

5.5 Hypothesis Outcomes

Following the descriptive testing above, there are a number of hypotheses that were tested in order to determine the overall relationships between the data and the findings. The hypotheses were posed based on elements of Research Question 4 ("What are the differences in fraud management between Kenyan and international banks?") although they refer to specific elements of the corporate governance and other elements of the bank. For more information regarding the theoretical foundations of the hypotheses, please refer to Section 2.8, Chapter 2. These elements are primarily based on internal elements and characteristics of the bank, particularly size and organization, as is consistent with the conceptual framework (Chapter 3, Section 3.10).

The hypotheses that underpinned this study are listed in Table 5.20. It is theoretically impossible to prove that a research hypothesis is true by statistical analysis, however, it is possible to disprove a null hypothesis (i.e., infer that it is not true) at a prescribed level of probability (Field, 2009). Consequently, the research hypotheses were converted into null hypotheses for purposes of statistical analysis. Each null hypothesis (H_0) proposed that the results were not statistically significant (i.e., the data were inconsequential, because they were caused by random chance). The variables extracted from the questionnaire item scores which were used to test the null hypotheses are defined in Appendix IC

If a null hypothesis was rejected, then the corresponding research hypothesis could be accepted, because it was unlikely that the data were caused by random chance. If the null hypothesis was not rejected, then the research hypothesis was redundant, and nothing meaningful could be concluded.

Table 5.20 – Research and Null hypothesis

Research Hypothesis	Null Hypothesis
1a. The total size of the loss to fraud will vary directly in proportion to the type or scope of the bank.	$H_0$1a: The value loss to fraud is not significantly associated with the type of bank
1b. The loss to fraud as a percentage of annual earnings will vary depending on the size of the bank.	$H_0$1b: The percentage loss to fraud is not significantly associated with the size of bank
2a. Banks that are international banks or international subsidiary banks will be more likely to use criminal prosecution or civil action against fraudsters than national, regional, or local banks.	$H_0$2a. The type of action used against fraudsters is not significantly associated with the type of bank
2b. Banks will be more likely to use criminal and civil action against external parties than against internal parties.	$H_0$2b. The type of action used against fraudsters is not significantly associated with the type of party
3a. The use of procedural and auditing approaches to fraud detection and monitoring will result in lower occurrence of fraud.	$H_0$3a. The type of security protocol is not significantly associated with the detected fraud (%)
3b. Larger organisations will be more likely to adopt organisational security protocols than smaller organisations.	$H_0$3b. The type of security protocol is not significantly associated with the size of the bank

5.5.1 Hypothesis 1

Research Hypothesis 1a and 1b were tested using the bank coverage (local to international) as the scope variable (the independent variable). The dependent variables were the total loss due to fraud and loss to fraud as a percentage of annual earnings. These variables were tested individually. This was tested at a confidence level of $p = 0.05$ using the χ^2 test statistic.

Research Hypothesis 1a

Hypothesis 1a: The total size of the loss to fraud will vary directly in proportion to the type or scope of the bank.

$H_0$1a: The value loss to fraud is not significantly associated with the type of bank

25 respondents reported the value of their loss to fraud. As the typical loss reported was about KES 5,000,000 the value loss to fraud was collapsed into <KES 5,000,000 and > KES 5,000,000. In so doing not more than 50% of the cells in the cross-tabulation were less than 5. The null hypothesis was not rejected, indicated by $p > .05$ for the χ^2 test statistic (Table 5.21) implying that Research Hypothesis 1a was rejected. There was no significant association between value loss to fraud and the type of bank.

Table 5.21Cross-tabulation of value loss to fraud x type of bank

VALUE LOSS TO FRAUD (KES)	TYPE OF BANK		Total	χ^2 test statistic	p-value
	National/Local/ Other Bank	International Bank/Subsidiary			
< 5,000,000	11	3	14	.682	.409
>5,000,000	7	4	11		
Total	18	7	25		

Research Hypothesis 1b

Hypothesis 1b: The loss to fraud as a percentage of annual earnings will vary depending on the type or size of the bank.

$H_0$1b: The percentage loss to fraud is not significantly associated with the size of bank

The same process used under Hypothesis 1a was repeated using the size of the bank (number of employees) as the independent variable. 56 respondents reported their percentage loss to fraud. The percentage loss to fraud was collapsed into < 1% and > 1% so that not more than 50% of the cells in the cross-tabulation were less than 5. The null hypothesis was not rejected, indicated by $p > .05$ for the χ^2 test statistic (Table 5.22) implying that the Research Hypothesis 1b was rejected and that there was no significant association between percentage loss to fraud and the size of the bank.

Table 5.22 Cross-tabulation of percentage loss to fraud x size of bank

PERCENTAGE LOSS TO FRAUD	SIZE OF BANK		Total	χ^2 test statistic	p-value
	<500 employees	> 500 employees			
< 1%	21	27	48	.108	.742
>1%	4	4	8		
Total	25	31	56		

While the χ^2 test statistic did not yield a significant result, the earlier analysis based on bank size determined that there was a significant difference in the overall turnover lost to fraud in the past year (Table 5.3, Section 5.3.2). Examination of medians by size of the bank reveals that banks with under 100 employees (N = 4) experienced a mean loss of 0.775% (standard deviation 0.608); banks with 101 to 500 employees (N = 9) experienced a loss of 1.036% (standard deviation 0.628); banks with 501-1000 employees experienced a loss of 2.0667% (standard deviation 1.613); and banks with 1,001 to 10,000 employees (N = 24) experienced a mean loss of 1.0425% (standard deviation 0.35613). Thus, banks with between 500 and 1,000 employees are significantly more likely to experience relatively higher losses than other groups.

Given these findings, *Hypothesis 1b* is rejected but could be viewed as a moderate relationship, as banks with over 500 employees did experience a higher loss than other banks. There was no significant relationship between fraud and turnover/value loss. Thus Hypothesis *1a* is rejected.

These findings are somewhat inconsistent with previous findings (Murphy, 1993; Barnes and Webb, 2007). Reasons for inconsistency could involve the relatively smaller sample size used for this research compared to previous researches that have used large samples; limitation to a single industry – other researches have involved several industries while this study has only considered one industry; differences in category definition of employee size and general differences in the Kenyan business structure.

5.5.2 Hypothesis 2

Hypothesis 2a: Banks that are international banks or international subsidiary banks will be more likely to use criminal prosecution or civil action against fraudsters than national, regional, or local banks.

$H_0 2a$: The type of action used against fraudsters is not significantly associated with the type of bank

The total number of actions taken by the banks against fraudsters was 80, of which 60 were criminal and 20 were civil prosecutions. The null hypothesis was not rejected, indicated by $p > .05$ for the χ^2 test statistic (Table 5.23) meaning that international banks or subsidiaries will not be more likely to use criminal prosecution or civil action against fraudsters than other types of banks. There was no significant association between the type of action used against fraudsters and the type of bank.

Table 5.23 Cross-tabulation of action used against fraudsters x type of bank

ACTION	TYPE OF BANK		Total	χ^2 test statistic	p-value
	National/Local/Other Bank (Internal and External 1st and 2nd Parties)	International /Subsidiary (Internal and External 1st and 2nd Parties)			
Criminal	46	15	61	.023	.879*
Civil	14	5	19		
Total	60	20	80		

Hypothesis 2b: Banks will be more likely to use criminal prosecution or civil action against external parties than against internal parties.

$H_0 2b$: The type of action used against fraudsters is not significantly associated with the type of party

Criminal or civil action was taken against 80 fraudsters, of whom 42 were external 1st or 2nd parties and 38 were internal 1st or 2nd parties. The null hypothesis was not rejected, indicated by $p > .05$ for the χ^2 test statistic (Table 5.24). Therefore Research Hypothesis 2b is rejected as there was no significant association between the type of action used against fraudsters and the type of party.

Table 5.24 Cross-tabulation of type of party and type of bank

PARTY	BANK		Total	χ^2 test statistic	p-value
	National/Local /Other Bank	International /Subsidiary			
Internal (1st & 2nd)	30	12	42	.051	.821
External 1st and 2nd)	28	10	38		
Total	58	22	80		

Hypothesis 2a compared total prosecution against internal and external perpetrators (dependent variable) based on the categorical variable of scope of the organisation. The χ^2 test does indicate that the probability of prosecution is not higher in international banks compared to other banks, failing to support the views of Fisher et al (2001) on the possible positive effect of incentives and rewards on disclosure and subsequent prosecution of fraud. This result also fails to support the views expressed by Abiola (2009) on the likelihood of Nigerian banks to avoid using prosecution.

Hypothesis 2b addressed the likelihood of prosecution against internal and external actors. The results of the chi-square showed that distribution of internal prosecution was not significantly different from expected. Likewise, there was no significant difference in expected distribution among the external prosecution test. Given this evidence, hypothesis 2b is rejected, and banks are equally likely to prosecute internal as well as external perpetrators.

Due to the small sample size only two categories were used for this hypothesis (International banks and other banks). The results may perhaps have been different if the

sample was large enough to allow more categories - local, regional, national and international banks.

5.5.3 Hypothesis 3

Hypothesis 3a: The use of procedural and auditing approaches to fraud detection and monitoring will result in lower occurrence of fraud.

$H_0$3a. The type of security protocol is not significantly associated with the detected fraud percentage.

The null hypothesis was not rejected with respect to seventeen of the protocols, indicated by $p > .05$ for the χ^2 test statistics (See Appendix ID). There was no significant association between these types of security protocols and the percentage of detected fraud. The null hypothesis was, however, rejected with respect to two protocols, specifically (a) Training employees on fraud prevention ($\chi^2 = 4.873$, $p = .027$) and (b) Establishing a fraud budget ($\chi^2 = 11.370$, $p = .001$). Statistical evidence is provided to indicate that these two security protocols were significantly associated with the percentage of detected fraud. This signifies that there is weak acceptance for the outcome and largely there is no significant association between the use of certain preventive measures and the level of fraud. Results are included in Appendix ID

This finding is important as it supports research by Barnes and Webb (2007) who found that the nature of management controls were not significant in determining either the size of fraud loss or the susceptibility of the organisation to fraud or theft.

Hypothesis 3b: Larger organisations will be more likely to adopt organisational security protocols than smaller organisations.

$H_0$3b: The type of security protocol is not significantly associated with the size of the bank

Hypothesis 3b proposed that relatively larger organisations were more likely to use organisational protocols than relatively smaller organisations. Relatively smaller organisations are defined as those with fewer than 500 employees

The null hypothesis was not rejected with respect sixteen of the protocols, indicated by $p > .05$ for the χ^2 test statistic (See Appendix ID). There was no significant association between these types of security protocols and the size of the bank.

The null hypothesis was, however, rejected with respect to three protocols, specifically (a) Establishing an ethical code of conduct ($\chi^2 = 4.873$, $p = .027$); (b) Ethics training ($\chi^2 = 3.958$, $p = .047$); and (c) Close supervision ($\chi^2 = 5.939$, $p = .015$). Statistical evidence is provided to indicate that these three security protocols were significantly associated with the size of the bank (Appendix ID).

This again indicates that, although this hypothesis cannot be rejected entirely, there is only weak support for its outcomes agreeing with research by Barnes & Webb (2007).

5.6 Reflection on the Research Questions and Conceptual Framework

Research Question 1 asks "What are the characteristics of fraud in the Kenyan banking industry?" The findings reveal that a majority of the respondents' view that fraud is a major problem in Kenya's banking industry. There is a likelihood that fraud will continue to increase in the financial sector with the banking industry likely to witness an significant increase in the short and long term mainly due to economic pressures within the country, advanced computer technologies (like internet banking), more sophisticated criminals (like hackers), ineffective justice systems, changing societal values among others. Fraud largely comprised of theft of cash, diversion and misappropriation of cheques and card fraud by manipulating computer systems and through identity fraud. Fraud losses are estimated mostly at less than 1% of the turnover of the respective banks with a few banks reporting losses of between 1-5%. Using Chi square tests the study established that there was no significant relationship between the type of security

protocol and the amount of fraud loss. Statistical tests also showed that there was a weak association between the types of security protocols and the size of the bank (Hypothesis 4).

Research Question 2 considered "What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?" The research findings show that perpetrators of fraud were not limited to one category or group of people. Majority of fraud is committed through collusion of internal (employees and managers) and external (customers, criminals, organized criminals, former employees etc.) parties. Perpetrators were relatively young (31-40 years) and mainly male. He or she is most likely involved with the bank in a managerial or cash-handling non-supervisory role, and if there are external colluders they are likely to be customers of the bank. Most frauds are collusions rather than individual acts, indicating that fraud perpetrators are likely to work in groups. The main factors that motivated perpetrators to commit fraud as perceived by the respondents stemmed from the existence of an opportunity to commit fraud, lifestyle habits, personal financial pressure and simple greed. Fraud opportunities come in the form of poor internal controls, overrides of internal controls by management and poor screening procedures in the recruitment and selection process. The perpetrators advanced justifications or rationalizations ranging from "it was a way to get rich quick", "others were getting away with it", and "there was a need due to family pressure", among others, as a way of mitigating their fraudulent actions.

Research Question 3 sought to find out "How do banks approach fraud management?" This question has been answered through various views that considered fraud prevention, detection and investigation methods, actions resorted to by banks on discovering fraud, software usage and organizational responses to fraud. One third of fraud is detected by accident implying that fraud management partly relies on chance discoveries of fraud. The respondents also identified internal controls as a way through which fraud is detected. Investigation of fraud is primarily carried out internally by the security departments but there is also the involvement of law enforcing bodies in fraud investigation. This may imply that banks do report fraud cases to law enforcement bodies.

In attempting to manage fraud banks responded by taking action against both internal and external parties, immediately dismissing internal parties and following this up with criminal and civil prosecution, while the main response for external parties was criminal prosecution, followed by civil prosecution. It is rare that banks recover any funds or assets traceable to fraudulent activities.

Ranking by respondents showed that organizational measures often adopted to enhance the prevention of fraud were: the improvement or review of internal controls, the use of fraud prevention training, the use of fraud prevention policies, the use of an ethical conduct code and the use of a fraud hotline. Organizations used at a minimum two types of software security protocols. The least used security protocols, digital analysis, discovery sampling and data mining were found to be the most effective fraud prevention and detection security measures. However, further analysis using chi square cross tabulation (Hypothesis 4) revealed that there was no association between the fraud levels and the number of software solutions used.

The last research question poses “Are there differences between the approaches to fraud management used by Kenyan and international banks?” This question has been partially answered in this chapter through the various hypotheses outcomes. Statistical testing on Hypothesis 1 has shown that there is no significant relationship between the type of bank and the amount of fraud loss. There was also no significant relationship between the size of the bank (as measured by number of employees) and the extent of fraud loss. Using Chi-square tests Hypothesis 2 established that international banks or international subsidiary banks were not more likely to use criminal prosecution or civil action against fraudsters than national, regional, or local banks. There was also no significant association found between the type of action used against fraudsters (criminal and civil prosecution) and the type of party (internal and external parties). However, the descriptive statistics does show that international banks have a higher count in terms of pursuing prosecution compared to the other types of banks. This perhaps shows a greater willingness of international banks to prosecute fraud.

Sections 5.4.1 and 5.4.3 can be considered in relation to the focal part of the conceptual framework labelled “Fraud” (Chapter 3, Section 3.10, and Figure 3.2). This aspect of the conceptual framework is captured through the discussions in Sections 5.4.1 and 5.4.3 on the nature and characteristics of fraud. The findings in this chapter also have implications that relate to the central part of the conceptual framework. The individual perpetrator is at the centre of the fraud, symbolized by the fraud triangle. The fraud triangle in the conceptual framework has been illustrated through the findings and discussion in Section 5.4.2 which has highlighted who perpetrates fraud, what are the perceived motivations (pressure) for committing fraud, what are the organizational loopholes (reasons) that present an opportunity for fraud to occur and what are the justifications or rationalizations used by the fraudsters to mitigate their fraudulent acts.

Section 5.4.4 on organizational responses to fraud directly relate to the internal industry environment depicted on the conceptual framework. This section has focused on the prevention, detection and investigation of fraud which are areas of internal control systems. Hypothesis 1 has also addressed the relationship between the size and the type of the bank and the amount of loss. This can be linked to internal industry factors on the conceptual framework as it deals with the organizational characteristics (size and structure). Hypothesis 3a examines the relationship between the fraud prevention methods used and the amount of fraud which has to do with an aspect of internal industry, that of internal control and systems measures. Hypothesis 3b also touches on the internal industry factors as it concerns the relationship between organizational security protocols and the size of the bank.

Hypothesis 2a and 2b fit in the external industry factors as it focuses on prosecution which is a legal issue. Actions and outcomes pursued under Section 5.4.4.3 is also linked to aspects of law enforcement which again is part of legal and regulatory matters external to the industry.

5.7 Summary of Findings

Overall trends indicate that banks about 0.01% of their turnover to fraud in the past year with a mean of about 1.18%, or about 21,641,000 KES (approximately US$ $277,000 or €224,000 as of May 14, 2010). As banks grew larger, losses as a percentage of annual revenue grew smaller. This did not show a normal distribution; however, precise figures were not provided by all banks, and there was one extreme outlier that affected the analysis. Most respondents felt that bank fraud was a major issue that was increasing in importance.

Collusion between internal and external perpetrators was the most common type of fraud. The most common targets were cheques and cash, which were most commonly stolen or misappropriated. Detection was uncertain, with 33% of frauds being discovered by accident and 18% being caught by internal controls. Dismissal and criminal prosecution were the most common actions taken against fraudsters. Internal control reviews and training employees in fraud prevention were the most common responses to discovery of fraud within the organisation. The most commonly used technological prevention and detection techniques included anti-virus software, password protection, continuous auditing, and filtering.

The outcomes of the hypothesis testing are summarised as follows. Only five statistically significant associations were identified at the .05 level of significance, emphasizing the importance of certain security protocols with respect to preventing bank fraud. There was a significant association between the percentage of detected fraud and two protocols, specifically the training of employees on fraud prevention and the establishment of a fraud budget. There was a significant association between the size of the bank and three protocols, specifically establishing a code of conduct, ethics training, and close supervision.

No other statistically significant associations were found between the variables measured using the questionnaire. This may have been due to the relatively small sample size of 60 respondents, which compromised the statistical inferences. According to Cohen (1992)

the minimum sample size for a Chi-Square test using a 2 x 2 cross-tabulation at $\alpha = .05$ is 87 cases to detect a medium effect, increasing to 785 cases to detect a small effect. The sample size used in this study was therefore lower than the minimum necessary to obtain precise statistical inferences using a Chi-Square test to detect small to medium sized statistical associations at the 0. 05 level. Consequently, if this research is repeated in the future, a larger sample size, collecting data from more banks and respondents, is recommended.

Chapter 6
Qualitative Study Findings

6.1 Introduction

This chapter presents selected extracts from raw data gathered through field interviews which has been analysed and structured to provide some meaningful information. These extracts form the basis of themes that are to be discussed later in the Chapter 7. Seventeen interviewees were selected using snowball sampling. Each interviewee represented a different bank and was chosen from a cross section of large, small, public, local, national, regional and international banks operating in the capital city of Kenya, Nairobi within constraints of availability and access to interviewees. Methods of interviewing are discussed in Chapter 4 (Research Methodology).

This chapter discusses findings structuring them in terms of the conceptual framework. The findings of this qualitative study are arranged in the three main tiers of the conceptual framework: the perpetrator, the internal and the external environmental factors. The findings relate to the central part of the conceptual framework (Figure 3.2, Section 3.10) on the perpetrator – collusion and the Fraud Triangle (Section 6.2); the second aspect of the conceptual framework which includes internal bank factors with emerging themes on internal controls, fraud prevention and detection (fraud budgets, fraud detection and customers in fraud detection and adequate deterrence), internal industry-wide factors – information sharing, inter-bank competition and information technology (Section 6.3); the third aspect of the conceptual framework, the external factors findings are presented in Section 6.4 with themes on ethical issues, structural and institutional issues as well as cultural, socio-economic and information technology issues. Section 6.5 presents other issues arising from the interviews. Implications of these findings for the research questions and the conceptual framework are discussed in Section 6.6. A summary (Section 6.7) concludes this chapter. A sample transcribed interview can be found in Appendix IV and a list of interviewees in Appendix V. The qualitative study mainly addressed Research Questions 2 (“What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?”) and Question 3 (“How do banks

approach fraud management?") These questions are also addressed in the quantitative findings (Chapter 5) and will be discussed for integration further in Chapter 7.

6.2 The Perpetrator

The interviewees were asked to recall a recent fraud incidence that was typical and speak about it. Some of the characteristics and nature of fraud came through the interviews as a result of this. First, the types of fraud committed varied widely with the most common fraud being direct theft of cash from customers' accounts, followed by cheque frauds. Identity fraud was used in a majority of the fraud cases reported by the interviewees. All except two of the cases were reported to the police. One of the cases that were not reported to the police was contracted out to external private investigators. The average fraud loss was KES 5,000,000 (approximately £41,667 or USD 64,000). From the interviews it was evident that recovery of fraud funds was rare with only one interviewee reporting full recovery of stolen funds. Direct costs of investigation involved costs towards accommodation, fuel and time taken during the investigation. These findings concerning the characteristics of fraud support the findings from the quantitative study.

Like the quantitative study the average age of the perpetrator lies in the 31-45 years age bracket and perpetrators were mainly male. However, it is worth pointing out that there were a significant number of female perpetrators. Where the fraud involved an insider, the perpetrator typically held the position of a cashier, a teller or clerical staff in the bank. In at least four of the fraud cases the fraudsters had only worked in the bank and been in their current position for a period of less than two years which is a relatively short period of time.

The interviews followed up on possible fraud motivations as well as factors giving rise to fraud opportunities. The interviewees spoke of financial pressure as being the main fraud motivator followed by opportunity, peer pressure and greed. Again this closely agrees with the findings of the survey (Chapter 5). Apart from these known motivations one or two fraud cases recounted by the interviewees had motivations that were rare such as the

perpetrator being blackmailed and therefore stealing funds in order to make the payments. The factors that contributed to fraud and therefore presented fraud opportunities included weak internal controls, lack of segregation of duties and lax supervision. Internal controls were not only weak but they were ignored and not properly managed by the bank employees and management.

Based on the interviewees' fraud experiences the perpetrators behind a majority of the fraudulent acts were either insiders (employees or managers) or insiders in collusion with outsiders (mainly customers). Of the seventeen interviewees there were only three incidences of external fraud that involved only outsiders. Even then in one of the three cases involving outsiders one of the external fraudsters was an ex-employee who had insider information.

From the interviews the significant themes that can be identified with the perpetrator are the issue of collusion and the fraud triangle. The interviews confirmed that the elements of the fraud triangle were significant and this reflected through the findings on opportunity, motivations and rationalizations. In terms of the research questions collusion and the fraud triangle are part of the question on the characteristics of the perpetrator. Conceptually in the framework the fraud triangle represents the perpetrator and is positioned at the center of the conceptual framework. The findings on the two themes of collusion and the fraud triangle are discussed further in the sections below.

6.2.1 Collusion

The study revealed that one of the issues facing the industry was the problem of collusion between two or more individuals. Question 3 in the interview schedule sought to clarify who the perpetrator was and further in Question 4 whether the perpetrator acted alone, with internal and/or external collusion. A majority of fraud cases recalled by the interviewees involved fraudulent withdrawals made from customers' accounts either by or with the help of internal staff. The major themes that emerged from this included the

prevalence of internal control fraud and the problem of collusion and conflict between depositors and employees.

As one interviewee conceded *"it is difficult for an external party to defraud a bank without the help from an internal person" (Joseph – Local bank),* emphasizing the view that external parties rarely get involved in fraud on their own without support or help from an insider. This was further evidenced by a fraud incidence narrated by another interviewee, Ruth, an employee of a regional bank. Ruth described the role of the employee in finding external information, instructing the external perpetrator on how to overcome controls, and the importance of the position of the employee colluding within the bank. She noted that:

"The person who was responsible for making such changes failed to call the customer on the old telephone number and went ahead to change to the fraudsters telephone number. So that is where the catch was. After that was done everything else passed because any check you are calling to confirm you are confirming with the same fraudster."(International bank)

This case shows illustrates how employees who are entrusted with information and responsibility act in breach of the trust endowed on them when they divulge the same to other parties with the intention of defrauding another individual. They are aware of the systems and controls and instead of safeguarding these some of the internal people use their knowledge to perpetrate fraud against the organisation. The second thing that we can pick from this incidence is that fraud is encouraged by negligence on the part of the employees. The fact that a member of staff failed to make a critical telephone call is evidence that failing to implement internal measures can result in fraud losses. However, from the case above it is unclear whether the employee charged with the responsibility to confirm changes to telephone numbers was an integral part of the collusion.

Collusion is not easy to detect or to prove. Elijah (International bank) recalled a case where the main perpetrator was external; however: *"it could be possible there was internal collusion but that has not been proven."*

It is especially difficult to detect fraud when it is committed by a team or group of persons working together both on the inside and from the outside of the organisation. The creation of syndicates and cartels between the employees and external parties was a concern to Moses (International bank), who recalled a case where five members of staff, including cashiers, were involved in a single fraud.

Given that collusion is a main ingredient in the commission of fraud taking steps to detect or deter it is central to the fight against fraud. Establishing internal control systems that are effective is one of the ways to do this. Internal control systems are discussed in the Section 6.3.1.

6.2.2 Fraud Triangle

Following up on the quantitative study the interviewees were asked about two aspects of the fraud triangle, the motivations (pressures) of the fraudsters and the opportunities that facilitated the occurrence of fraud. Jacob (Local Bank) commented that the perpetrator had a *"…financial pressure. She thought she could multiply the money through some pyramid scheme that was promising a 50% return per month!"* This not only shows that the perpetrator was motivated by some kind of financial pressure but that she also rationalized that she could *"get rich quickly"* by investing the stolen funds in a pyramid scheme. Participants Moses, Joseph, Simon all explained the fraud motivation as being financial pressure. The interviewees also pointed out that sheer opportunity and greed were motivators. Participants Joel, Thomas, Simon spoke about opportunity being the motivator; while Ruth and Paul made reference to greed, lack of ethics and an extravagant lifestyle as motivators. An example of this is shown in the statement below:

"Though she had only worked for a short time with us this person had worked for two years in other institutions. With this kind of experience and the fact that she had forged documents it was not surprising that she could commit fraud – so she just took advantage of an opportunity" (Thomas, Regional Bank)

A motivator like peer pressure was also advanced in the fraud cases explained by Adam and Paul. The findings on motivators indicate that though fraud is motivated by various reasons, opportunity, financial pressure and greed seem to be the main motivators.

Considering fraud opportunities the interviewees were asked to explain the factors that contributed to or facilitated the occurrence of the fraud episode. The main three factors that were mentioned were poor or weak internal controls, the problem of separation of duties and poor supervision.

By way of examples, Moses (International bank) and Joseph (Local bank) both explained that the failure to separate the making of the application and checking of the application resulted in the fraud occurring while Gabriel (Regional bank) put the fraud down to ignoring internal controls as well as the lack of a separation of duties. Like Gabriel, Joel (Regional bank) said that poor internal controls were in place allowing the fraud to occur. David (Local bank) and Thomas (Regional bank) indicated that a lapse in supervision presented a fraud opportunity:

"The supervisor did not play her role in inducting the employee on payment procedures when she joined and also the supervisor did not play her role in authorizing the payments that were above the teller limit. So I would say procedures were not followed and supervision was lax." (Thomas, Regional Bank)

The findings in this section show that the Fraud Triangle elements have been identified through this study and these will be discussed in greater detail in the next chapter. The fraud opportunities create a challenge mainly to the internal control systems of organizations. More findings on internal controls continue in the next section.

6.3 Internal bank and Industry Factors

The second aspect of analysis within the conceptual framework is that of internal factors. As discussed in the literature review (Chapter 3, Section 3.10.2, and Figure 3.3) the internal factors have been separated into two: internal bank specific factors (Internal

Controls & Systems, organizational characteristics and insider involvement) and internal industry-wide factors (inter-bank competition for customers and information sharing). The internal bank specific factors are discussed under Sections 6.3.1 and 6.3.2 while internal industry wide factors are discussed in Sections 6.3.3. Notably sub-section 6.3.3.3 on Information Technology is part of both the internal and external industry factors. For this research it will be discussed under the internal industry-wide factors.

Respondents were asked some questions that related to fraud management and these responses were later categorized under various dominant themes which are discussed below. Section 6.3 therefore mainly addresses Research Question 3 ("How do banks approach fraud management")

6.3.1 Internal Control Systems

After talking about their fraud cases, the interviewees were asked the questions "What did you learn from this incident?" (Question 5 on interview schedule) and "What could be done to prevent the fraud from occurring again" (Question 6 on interview schedule).

Narrating his experiences and lessons learnt from fraudulent activities Jacob stated that:

"We learnt that we have to strengthen our internal controls, so that no one single person can post and withdraw money without consent from a second party." (Local bank)

The separation or segregation of roles and duties was cited as being a useful tool of internal control. One recent innovation used by banks to attract customers is unsecured loans of up to KES1 million (USD12,900). Moses (International bank) explained how they suffered a loan application fraud because of a lack of clear separation between the "maker" of a document and the "checker" of the same; that is, the same person made out the application and performed the background and credit checks, offering the opportunity for fraud. After the fraud occurred, internal controls were improved to prevent this from happening again.

By segregating duties the management uses one individual to act independently as a check or balance against another. Using staff rotation is another approach identified by the banks for this purpose. Rotation ensures that employees take up different roles, duties and responsibilities and perhaps in the process re-shape relationships, effectively breaking up collusion. One regional bank manager, Gabriel, states the importance of this for senior officers. He stated that managers held positions for no more than two years, and then were rotated, as were their immediate superiors and subordinates. Short-term reassignments to different regions were also used. However, this was not universally successful, with some fraudsters using job rotation to confuse new staff members.

The findings of this study revealed that collusion poses a daunting challenge to the internal controls put in place by individual banks. The insider is aware of what and where the controls are and how to circumvent them. Therefore, having controls in place is not enough to fight fraud, the controls also need to be followed and enforced by those in position to do so. As Ruth (Regional bank) commented, fraudsters often beat the system and it is important *"… not to over trust staff."*

The controls must also be working at all times. As Joseph, an employee of a local bank observed any lapse in controls increases exposure to fraud. In his estimation, strong controls sometimes lead to relaxation of observance, which can open the bank to more fraud. Simon said his bank had learnt that it is possible to manipulate controls and as such the internal controls should be reviewed constantly:

"Controls can be manipulated. We must at all times review our controls. We also learnt that there must be checks and balances… every member of staff does have a price and critically it is the controls that are really important." (International bank)

Caleb reinforced this view:

"Fraud and fraud prevention….all these things begin with individuals, boils down to an individual."(Local bank)

Overcoming low integrity thresholds among the staff remains a challenge in tackling collusion and in bolstering internal controls.

While strengthening internal controls reduces exposure to fraud, it can also cause problems. Excessive controls can dampen customer service as further requirements are placed on customer transactions. This requires a balance between strong internal controls and customer service, and banks cannot eliminate all risk. Thomas states:
"We usually learn from experience….where a fraud penetrates the measure we have put up. So we will beef up the measure or control and review it. If it is inadequate we add more controls. But we also don't want to put up stringent controls that will hamper service. So we have to bear with some risk."

It is not only poor internal controls and overrides of internal controls that should be considered. The interviewees identified the importance of tightening screening procedures during the recruitment of new employees. Speaking with interviewees highlighted the fact that one of the causes leading to fraud was complacency during the phase of recruiting new employees - due processes were not being followed before the recruitment of new staff. Therefore they had learned through their fraud experiences the importance of carrying out effective background checks on employees.

Ruth (Regional bank) expressed that while firms must carefully select and screen employees, this did not always happen. In one case of fraud at her bank, Ruth revealed that the perpetrator had personal debt and financial management problems known to her former employer. Ruth's bank hired her without sufficient background checks or references.

In about half the cases that involved internal perpetrator(s), the perpetrator was known or later discovered to have had a fraud history. This raises an important issue about the quality of background checks carried out, if any, by the banks and how effective these checks are in minimizing fraud. However, these were not entirely attributable to banks.

Thomas (Regional bank) indicated that delayed responses caused problems. In one case described by Thomas, an internal perpetrator forged university credentials. The employee

was hired before references were returned, and employers did not give poor feedback "*as they fear being sued for libel in event of any wrong information being given."* The employee worked for the bank for two months, perpetrating fraud, before the university indicated that they did not have a student by that name.

Adverse reports concerning the behaviour of staff members should not be taken lightly while doing background checks. Gabriel (Regional bank) recounted a case where there were rumours regarding a fraud perpetrator that were not followed up, reducing the ability to avert fraud. Later, they learned that one of the perpetrators of fraud in their bank did have previous history of fraud. Joel (Regional bank) and Thomas (Regional bank) agreed with Gabriel that background checks were vital and should not be ignored, and that these should be done prior to employment.

Therefore, arising from the interviews is a concern about the efficacy of recruitment policies in fraud prevention. Why some banks are hiring employees without carrying out appropriate background checks given the fraud risk involved is a thought provoking issue.

This Section, 6.3.1, has raised some important findings that relate to internal controls and screening procedures and their importance in fraud prevention. These are lessons that have been learnt through the experiences of the interviewees. When asked whether the fraud incidences had helped the organization to improve its fraud prevention and detection methods (Question 6 of interview schedule) all interviewees affirmed that the fraud incidents had helped the organization to improve their internal controls either through job rotation, segregation of duties, or carrying out appropriate background checks.

6.3.2 Fraud prevention and detection

To answer Research Question 3 "How do banks approach fraud management?" the respondents were asked whether their organization has a budget for fraud, the size of the

fraud budget as a percentage of the total organizational budget and whether this budget had increased over the past five years (Questions 13-15 of interview schedule).

Another theme that has emerged is the process of detecting and preventing fraud and the challenges that are faced by banks in this area. Respondents generally report a shortage of resources and uncertainty regarding resource assignment for fraud prevention and detection. Of particular concern are findings that the majority of frauds are detected through customer action (such as examination of bank statements) rather than through bank internal or external controls.

6.3.2.1 Fraud budgets

Fighting fraud is a costly affair. Organisations need to weigh the cost of fighting fraud with the benefits they will receive from reduced fraud. The cost of fraud prevention to the organisation will be determined by the trade-off between cost and benefit.

The size of the fraud budget can be an indicator of a firm's commitment to fight fraud. Of the banks surveyed in this study very few had actual information on the organisations fraud budget and could clearly state the same. Moses (International bank) and Joshua were in a position to confidently say that they had a fraud budget that could be used for staff training and materials, litigation, and information sharing. Joshua indicated this budget could be expanded on request: *"… every time there is an issue relating to budget the business has always given the money. So funding to fight fraud is there." (Joshua – International bank)*

Solomon (Local bank) gave a thorough run down of their fraud budget, indicating that key areas included prevention, information and investigation, intelligence (including money for tip-offs), prosecution and travel, bank security forums, and specialized officer training. This budget covered all branches of the bank.

One justification for lack of a fraud budget was that fraud was a sporadic event rather than a regular occurrence. Being a sporadic event there is less reason to make a specific

provision by establishing a distinct budget for it. As Caleb reasoned *"it is hard to plan for fraud as it is not anticipated. There are times you can go without fraud for even a year and there are times you encounter fraud several times within a given year. So due to the sporadic nature of fraud we do not specifically allocate any money for it."(Local bank)*

Another reason for not maintaining a specific budget was that in their opinion, the amount of money involved in most of the frauds was inconsequential. Adam stated: *"We have not really had significant levels of fraud to warrant a separate, distinct budget. The case I talked to you about was the one major case we have ever had. Most of the cases that occur occasionally involve small sums of money."*
This reflected an attitude that seemed to suggest that fraud is only significant if the amount involved is large and contradicts the general opinion that fraud is significant and increasing.

Even in the absence of a specific budget for fraud the bankers said they had the money to fight fraud. Caleb states, *"There are funds that are available to address fraud cases whenever they arise. The management is supportive and we have an open budget. I have never requested for money and been turned down. The money to fight fraud is there and it is enough" (Local bank)*

This gives the impression that some banks have endless resources to fight fraud. Whether this is sustainable at all times is debatable. It is clear that most banks may not spell out the actual amounts set aside specifically for handling fraud issues. In some cases fraud is masked under other budgets; Joseph (Local bank) indicated fraud was covered under the internal controls budget, while Thomas (Regional bank) stated his bank covered fraud under the operations budget. Both respondents justified this based on the unpredictability of fraud. Gabriel (Regional bank) indicated fraud was covered under the Information Technology (IT), due to the degree of fraud related to IT network vulnerability. David (Regional bank) explained that the fraud budget was met out of the audit department budget as the fraud department was in an early stage of development. These arguments

against budgets appear to imply that banks are simply responding to fraud or fraud attempts, using a reactive rather than proactive approach. In one exceptional case at a national bank, the fraud budget was withdrawn due to abuse by a bank officer; as a result the bank, according to Titus, *"only has a small allowance for investigators. It is very important and we have asked the management to restore it."(A National bank)*

Another question was what size the budget was as a percentage of total budget. There were few responses to this question, due to integration of the fraud budget or lack of budget. Moses (International bank) remarked that the fraud budget was not a significant amount in light of the total budget. According to him good control systems within the bank has frustrated a large amount of fraud resulting in a loss of only 1.7% when compared with the fraud exposure. Thus, *"when the budget is drawn based on previous year's budget the figure does not tend to be large…zero point something!"* Joshua (International bank) would not disclose an exact amount due to confidentiality, while Solomon (Local bank) indicated a ceiling of 0.2% of depositor liability for fraud prevention. Most respondents agreed that this amount had increased over the past five years, but did not give a specific figure; instead, they indicated that increased staffing in IT and internal auditing departments showed growth in spending. The increase was also attributed to "one-off" fraud sums that arise every year from unexpected fraud that *"really mess up the budget"(Moses – International bank)*. This statement belies the supposed unpredictability of fraud expenditures. Nonetheless there was also the perception that the introduction of new technologies has led to a decrease in the fraud budget or shifted it to the IT budget. However, Joseph (Local bank) indicated that his bank's cost controls resulted in a lack of increase, even though they could use it.

We can therefore note that there is an issue as to why a specific identifiable fraud budget should be planned for or if it should just be an ad hoc provision based on the reasoning that the occurrence of fraud is an unplanned event. It is also worthwhile considering why international banks appear to have embraced maintenance of specific fraud budgets before other banks.

6.3.2.2 Fraud detection and customers in fraud detection

As part of interview, question 3, respondents were asked to explain how the fraud was detected. The interviewees raised interesting points about how each fraud was detected. Some interviewees identified that whistle blowing had been useful in detection of the frauds as recounted below.

Ruth (Regional bank) recalled a case where an external whistle-blower alerted the bank to an imminent fraudulent withdrawal on a given account. Moses (International bank) recalled a case where an external whistle-blower using a fraud hotline alerted the bank to specific fraud on-going in 40 accounts; on investigation, this yielded over 300 fraudulent accounts. Joseph (Local bank) recalled a case where a relative of a bank employee provided information regarding the fraud.

There are also other sources of fraud detection. Staff rotation and the recruitment of new staff have also brought fraud to the front. Gabriel (Regional bank) noted a case where a new employee, after seeing a discrepancy between their own lifestyle and older employees, uncovered fraud. David (Regional bank) discussed a case where books did not balance after rotation of a staff member. However, internal controls were not effective. Most notably only one interviewee said that internal controls had helped to detect fraud, through end of day reconciliation. Adam (A National bank) indicated that one fraud, involving a stolen chequebook, was uncovered by the German police investigating the theft. Another indicated that a report in a local newspaper involving business corruption resulted in the bank investigating accounts and uncovering a fraud of millions of Kenya Shillings.

A majority of the fraud cases narrated related to fraudulent withdrawals from a customer's account or cheque frauds. The interviewees revealed that the customer was the first person to alert the bank to the incidences. Elijah, Abraham, Joel, Thomas, Joshua, Simon, and Caleb all reported similar instances where customers reported suspicious activity in their statements following cheque fraud or fraudulent withdrawals. In one other case, explained by Titus (A National bank), a customer complained after

asking for a balance in the bank, and being given a balance of approximately USD 10 rather than the expected USD 12,500. A cashier was found to have authorized withdrawals from this account as well as three other accounts. Without customer intervention these frauds may never have been noticed.

An important question was to consider what steps banks were taking to prevent and detect fraud. Top responses included training for employees and tightening of internal controls. Only one interviewee in the course of the interview mentioned that customer training was important in fraud detection:
"…the best effective tool is fraud training for all stakeholders - not only staff but also our customers. We also conduct fraud training for our customers as we did last month. We share with them what we think they did wrong or what they need to do or the frauds we think emanated from their end and what we want them to do."(Moses – International Bank)

If the customer in most cases is the person who detects the fraud then it makes sense that some time should be spent by the banks on increasing the customers' awareness and training. But this has not been the case in most of the banks. This issue will be discussed further in the next chapter.

6.3.2.3 Adequate deterrence

Interviewees were asked what kind of action the organisation took on the offenders. In majority of the cases the perpetrators were dismissed or had their services terminated and the organisation also went ahead to institute criminal charges by prosecuting them before a court of law. In some cases even though the perpetrators have been dismissed or arrested, the cases are still on going and unresolved. These actions are seen as deterrents to other fraudsters. However, there have been several cases where a person commits fraud in one organisation, is dismissed and later they re-join another organisation where they go ahead and still commit fraud.

This raises the question of whether dismissal as deterrent is effective. However, most respondents did believe that it was effective. Simon (International bank) recounted a case that was discovered through internal investigation, but where the courts required substantial IT documentation. This prosecution would have taken a long time, and the perpetrator was willing to recompense the bank. Simon believed that dismissal served as an example to others, and that they would not be re-employed. (Of course, given previous evidence this is likely not true.) Abraham, also from an international bank, felt dismissal was enough of a deterrent, showing other employees that they could lose their jobs.

However, some banks do use prosecution. Justifying the action of suspending, arresting and finally prosecuting the perpetrator, Thomas (Regional bank) said that his bank's zero-tolerance policy required prosecution as a deterrent to further crimes. Moses (International bank) indicated that his bank used dismissal, criminal prosecution, and a civil suit to recover funds lost as a deterrent. Jacob, Titus, and Gabriel (representatives from local, national, and regional banks) also agreed that dismissal *and* prosecution was appropriate deterrent.

Some interviewees had doubts about effectiveness of dismissal or prosecution. David did not think that dismissal and prosecution were an adequate deterrent as it did not deter perpetrators from re-offending and also due to corruption in the judicial system, citing that lengthy resolution of cases, technical complexity, corruption, and frequent acquittals made prosecution an inefficient deterrent. In David's words: *"As you know our judicial system takes long to resolve cases and there are cases being lost on technicalities…so we have seen many cases where people have been acquitted when they should not have been. We have taken many people to court but they continue committing the crimes. I would say that prosecution is just one of the ways to deter but certainly not an efficient one. Many people have several cases in court but they know they can buy their way out of court and they know the cases can be lost on technicalities; so they continue to commit fraud." (Regional bank)*

Solomon (Local bank) explained how they opted for a negotiated settlement one year into the arrest of the external perpetrators rather than pursue a conviction. This settlement resulted in the bank recouping some money and cutting short a lengthy criminal proceeding.

Some of the interviewees had mixed answers to the question on adequate deterrent. Adam (A National bank), recalling a fraud incidence that involved an off-shore cheque, said that while local perpetrators would be deterred, it was unlikely to work with international perpetrators. Joseph (Local bank) also felt that dismissal and prosecution were currently the best option. However, he did not think that it was an adequate deterrent as there is always the fear of the perpetrator re-offending. Like Adam and Joseph above, Ruth took a view that dismissal was necessary but perhaps not sufficient. Talking about a fraud case where the internal perpetrator was only dismissed, Ruth felt that upon dismissal a perpetrator should also be prosecuted.

Overall, dismissals and prosecution were not likely to prevent perpetrators from reoffending, though they may deter other employees. In particular, these strategies are not preventative. Exploring other approaches to preventing re-offense is discussed in Chapter 7.

6.3.3 Internal industry-wide factors

As mentioned earlier in Section 6.3, two key internal industry-wide factors, discussed below, is information sharing within the industry and inter-bank competition for customers. In the banking industry in Kenya, major issues that emerge are information sharing and competition for customers. In other words, the industry environment is based on a cooperation-competition model which potentially creates tensions and problems. In addition to these two factors, internal information technology factors will also be included for discussion.

6.3.3.1 Information sharing within the industry

Respondents were asked whether banks share about their fraud experiences at industry level (Question 8 on interview schedule) and what measures banks are putting in place jointly to reduce the incidence of fraud (Question 9 on interview schedule).

From the interview findings it emerged that there was a reluctance to share fraud information within the industry. Even where attempts are made to share information issues including public image and perception, historical precedent and at times management directives reduced the level of sharing. As one interviewee observed; *"…banks don't want to wash their dirty linen in public; they don't want to tell you how they have been hit by fraudsters. They want to keep it to themselves."(Gabriel – Regional bank)*

However, there is a growing trend towards information sharing due to increasing levels of fraud. The banks have learnt some lessons that have taught them that it does help to make a concerted effort at industry level to combat fraud. Adam mused:

"… now it is an industry norm that if this person hits one bank today, tomorrow it will be another bank. Apparently the perpetrator we are talking about had committed a similar crime in (Bank X) and another one in the (Bank Y). So we realized had we shared the information this person would not have succeeded in opening an account."(Adam – A National bank)

In a similar vein, Paul suggested:

"….if I circulated it to other banks, they would be able to take measures towards protecting themselves against an occurrence of a similar incidence within the industry… It would be my call that collaboration between industry players be encouraged; sharing of information on fraud should not be shunned; in fact should any institution fall a victim of fraud they shouldn't feel shy to share the same, because fraud is a common enemy to all banks and to all players" (Paul – Local bank)

Under the Kenya Bankers Association (KBA) a Securities and Fraud Committee was formed to handle issues related to fraud and banking security. This forum meets every month and ad hoc meetings are arranged when there are urgent issues to be discussed among the member banks. The research revealed that most respondents from international banks and national banks seemed to have a good knowledge of what goes on at the KBA. These respondents who were active participants of the Securities and Fraud Committee were conversant with how often the Committee met and what was shared. There were mixed responses from regional and local banks about the KBA. Some knew about the working of the KBA and there were a few who were aware about the KBA but had very little or no knowledge about it. Ruth had this to say:

"I am aware that there are industry meetings held by various representatives of banks and they share their fraud experiences but I have not been involved in one so I would not be able to tell you much" (Regional bank)

It is unclear whether Ruth was implying that her bank doesn't participate in the KBA meetings or if she meant that she personally was not involved. However, Ruth is a senior member of the audit department in her bank and the researcher would have expected her to be aware of the KBA even though she is not directly involved in the meetings.

However, Joshua suggested that the size of the firm could be a contributing factor to the level of active participation of banks. He explained, *"Most of the big banks have dedicated fraud investigators who come. But the smaller banks have managers who are appointed to look at fraud issues. When there are big issues we ask them to attend so they can know what is happening." (International bank)*

This inadvertently suggests that there is selectivity of membership participation and could explain why some banks are not as knowledgeable as others concerning the role of the KBA. To illustrate this further Abraham from a relatively smaller international bank had this to say in response to working with the KBA: *"Yes, but only if there is a big case. But we do share under the KBA. We get to know about the cases of fraud and they send out precautions and fraud alerts."(Abraham – International bank)*

The KBA is helpful in providing a forum where the bankers can share their experiences about present and emerging fraud trends so that the banks can learn from one another. Through the Association the bankers share issues of common concern to map out how best they can all move forward. One of the Regional bank interviewees talked of being able to network with fraud investigators from other banks through the KBA forum. Thomas, a regional bank employee, indicated that meetings were used for personal experience sharing and networking, and then forwarded the information on to other bank employees. Employees Paul (local bank) and Joshua (international bank) also supported the role of the KBA meetings for information sharing and networking.

Even though the Bankers Association is regarded as being helpful there is a feeling that the sharing mechanism is not well established or formalized. Bankers tend to share information in an informal way. Joseph thought that the Bankers Association was useful but he had this to add:

"…Unfortunately the forum (KBA) is not very well established for us as peers in the industry to exchange notes and find out who is doing what, how and where, or how they have been affected by a category of fraud. It is still currently at a personal basis…"(Local bank)

Caleb emphasizes that there is no established way of sharing information '*but as security managers we know one another and share informally…. even now if I have a fraud here at this time I will have to inform my other colleagues that there is this new trend in fraud that is happening. We are in communication but it is not formal, it is something between us as security managers of banks" (Local bank)*

From what Joseph and Caleb have said above, it appears that there is a great deal of camaraderie in the industry that allows free sharing of information in an informal way among the bankers. Given the history of reluctance in sharing information, an informal system is as far as some banks are willing to go.

The KBA could be instrumental in creating a strong alliance in the banking industry. By providing a common source of information the KBA can empower banks bringing change in the industry and strengthening fraud prevention and detection. In so doing the KBA can assert their role and position as an umbrella body so that every single banker, irrespective of their position in the bank, will be aware of the Association.

Sharing information remains the strongest joint measure being exercised by the banks. However, looking at one such joint measure banks have in place one comes across contrasting positions. Caleb seems to indicate that there is no common database or source of information on fraudsters.

"…we don't have maybe a database where we retrieve information….. we don't have something like that….But I remember one time when we met we did agree that we need to create a database where we can have all the fraud posted there…"(Local bank)

Still Paul implies that there is some kind of progress being made in setting up a database with images of fraudsters, but he actually does not say if this database has been implemented.

" … We are also in the process of coming up with a mechanism of sharing images or pictures of fraudsters, especially the most common ones because we have noticed that through the sharing of that information at that forum." (Local bank)

On the other hand Adam states that there is already a database in place:

"…we [i.e. banks] have set up a database that acts like a reference bureau where banks can make reference to individuals who are blacklisted. We share information now openly" (A National bank)

Caleb says, "*through the Kenya Bankers Association we are trying to come up with a data base of offenders/fraudsters and the new types and trends of fraud" (Local bank).*

Although these comments are confusing, it seems that there is not yet a central database. Some interviewees expressed hope that the KBA is in the process of developing a

database of fraud offenders. David (Regional bank) indicated this database was in progress, but not yet developed.

Sharing information has enabled the banks come up with common strategies that can deter habitual offenders. Thomas (Regional bank) indicated there were monthly forums were fraud was discussed, including credit card fraud. The industry has been able to compile some vital statistics on credit and debit card fraudsters, especially in regard to repeat offenders; according to Solomon *"….card fraud offenders are just the same people. We get to know the repeat offenders and we work towards prevention and when we get to know the repeat offender we can issue an alert and thus keep them out of the industry…" (Local bank)*

Interviewees also mentioned other useful measures KBA has taken within the industry such as organising trainings and workshops for the players in the banking industry. By bringing in experts the KBA releases new ideas and awareness of fraud for the banks. Adhering to the prudential guidelines and basic minimum standards set by the Central Bank of Kenya as measures of regulation can also go a long way in promoting a concerted effort on the part of all banks. Elijah (International bank), however, was of the opinion that the industry wide measures should be more preventive rather than curative, and that not much proactive activity occurred.

Respondents also indicated other joint measures, including a CBK Anti-Fraud unit operated by the police, but did not indicate these were a significant source of cooperation. Some reasons banks do not operate more formally or cooperatively could include costs, availability of time, different bank priorities and unwillingness to share or other reasons. Also of interest are the reasons as to why some banks are less aware and less active in the KBA. There is also a question about clarity among bankers on measures within the industry as illustrated by the difference responses on the availability of a fraudsters' database. In conclusion, KBA is going in the right direction but it is difficult to identify if KBA exercises selectivity that may be keeping smaller banks on the peripherals of information sharing or if it is a choice of the smaller banks.

6.3.3.2 Competition for customers

Another theme that emerged is the competition existing between banks for customers. This theme has come about as a part of the response to interview question 9 on the measures banks are putting in place to reduce the incidence of fraud. With just over 40 commercial banks available, bank customers in Kenya are spoilt for choice. This implies that banks have to compete fiercely to win and retain customers. To keep ahead of the competition every bank has to come up with new innovative services and bank products that will attract and retain customers.

Within the banking industry there is a popular policy referred to as "Know Your Customer" (KYC). As part of prudence the bank staff is expected to closely scrutinize any new customers applying to join the bank or any existing customer desiring to sign up for any of the bank services and products e.g. unsecured loans.

In spite of the apparent competition among the banks for new customers Adam (A National bank) explained that knowing your customer was important in reducing fraud, but said that *"you will find because we all want money, we are rushing to win any type of account…we don't even care about the document, because at the end of the day we are looking at the bottom line – what are your profits at the end of the year, hoping all is going to be well."* This comment shows that in a bid to increase the customer base and profits, procedures in account opening and customer transactions are at times not scrutinized properly. Furthermore, customers are often verified through relationships to other customers, according to Adam, which reduces the amount of information known. In Adams words "… *you see we eventually opened an account for him* (fraudster) *through our customer… but we didn't know much about this customer* (fraudster)*."(A National bank)*

Solomon agrees with the fact that you must not only know your customer, but controls and procedures must be complied with regardless of whom the customer is.

"Customers are not statistics, are we able to know them if we met in the streets? Cheque clearance standards have to be maintained, irrespective of who you are dealing with, whether it is a previous acquaintance or someone you are meeting for the first time…. If there is any discretion they must be in the interest of the bank and must be properly secured."(Local bank)

Seeking to know your customer will require due diligence to be taken before an account is opened. Caleb (Local bank), emphasizing this point, said that *"it is important to pay attention to due diligence when an account is being opened."* According to policy, customers need to give proof of where they live or operate from. Unannounced visits are made to the address given by the customer. Caleb added that staff also needs to be trained so that they are keener when opening new accounts and those who give recommendations should be scrutinized to ensure that they are legitimate.

This scrutiny of customers can be viewed as unnecessary by the customer and in effect act as a disincentive, pushing the customer away. Banks struggle between the pressures of customer demands and the KYC program requirements. As Joshua said:
"We should not allow competition between banks for customers to hamper fraud prevention." (International bank)

The banks need to find a solution that will strike an equitable balance between increasing the number of customers and amount of profits without exposing the banks to potential fraud risks arising from limited knowledge of the customers. This may require some kind of background checks on the customer such as credit rating, accounts held in any other banks, etc. Whether the banking industry is in a position to do this is a matter that needs to be discussed further in later chapters.

6.3.3.3 Information Technology - Use of fraud software and technology

Interview question 12 asked "How has the bank protected itself by the use of fraud software and technology?"

One of the ways that banks can secure their systems against external and internal attack from fraudsters is to employ protective software and computer technologies. Other than a few cases, most of the banks have taken specific measures to protect their networks. The most common tool used is firewalls, which block access to vulnerable systems and control access based on specific profiles. Banks have also used customer education; for example, they have warned customers about phishing attempts, in which fraudsters lure customers to fake bank Web sites to provide personal information. Joshua indicates that his international bank has an anti-phishing unit at the group level.

For internal protection banks are using passwords with restricted access rights. This way only a few people in the organisation have access to critical information, and the bank knows who can access the system. David indicates that usernames and passwords are associated with all actions within the system. However, officers are responsible for password security, and if this is breached it opens the bank up to risk.

People are an important element in the effective operation of fraud software and technology. Employing key resource persons and vetting to determine the right personnel is crucial. With the right personnel then you can set up policy statements and then set up the structures. Elijah commented that policies such as getting customer images and soft copies of the customer's signature are not IT-dependent, but are people-dependent; making sure these procedures work is crucial for security. Customer photos and signatures are also used by Thomas's regional bank as a fraud prevention measure. However, this means that banks need effective training for faked documents, signatures, and photos. Some banks also use software packages to protect against credit and debit card frauds. Simon indicated that his international bank uses the commercial Fraud Guard software package.

Issues of concern are whether banks are really setting up structures before using fraud technologies and how secure the systems are. International banks appear to be ahead of the other banks in technology. Some of the potential reasons for this could be due to cost

of required technology or expertise, economies of scale, increased exposure to fraud, or earlier entry into Internet banking than local, national, or regional banks.

6.4 External Industry Factors

The third aspect of the conceptual framework includes external factors that impact the levels of fraud and the fraud prevention and detection process. External factors include ethical, structural and institutional (legal and regulatory), socio-economic, cultural, technology and other external factors. All banks within this environment will be affected by the same factors. These external factors are discussed below.

6.4.1 Banking Ethics

Interviewees were asked various questions regarding banking ethics, including questions about codes of ethics and ethical culture. The responses were relevant to the socio-cultural aspects of the occurrence of fraud.

6.4.1.1 Code of ethics

Respondents were asked “Does your bank have a code of ethics and are all the employees aware of it?” and “Who is responsible for developing an ethical culture in the organisation?” (Questions 20 and 22 on interview schedule)

An emerging view from this research is that somebody should be charged with the responsibility of ensuring that there is an ethical culture within the organisation. An organisational ethical culture, if nurtured well, can have an impact on individual behaviour.

Most respondents said that Human Resources was responsible for development of ethical culture, while in some international banks this responsibility was shared between Ethics and Risk Management departments as well. The HR department is guided by the Director and other top managers.

Most of the interviewees responded affirmatively that their banks have a written code of ethics with at least half of them adding that the staff are required to sign the code of ethics as confirmation that they have read the code and are aware of its contents. In some cases the employees are expected to re-read the code and sign afresh every six months. However, there was no indication of follow-up to ensure respondents had integrated this code. Joseph and Titus (local and national bank respondents) indicated that their banks did not have codes of ethics or fraud policies. Both acknowledged that this was a problem.

6.4.1.2 Unethical Behaviour

Questions 21 and 23 on the interview schedule read "Has the organisation experienced any unethical behaviour in the past 5 years?" and "What type of unethical behaviour has the organisation experienced on a regular basis in the past 5 years?"

A majority of the interviewees admitted that the organisation had faced some cases of unethical behaviour. Such behaviour included staff dishonesty, accessing customers' accounts, divulging customer information, stealing cash, borrowing money without authorization, misusing sums of money intended to serve as "floats", and sexual harassment. However, most respondents indicated this was not usual.

Several examples were given. Adam indicated two cases where staff members had been found to be taking money from customer accounts, which resulted in a change of practice to frequent re-signing of the ethics policy (as well as dismissal of the staff members). Joel cited cases of cash theft and creation of fictitious transactions, while Joshua noted some cases of staff dishonesty.

Ethics policies were a major factor in preventing unethical behaviour. Simon (International bank) opined that constant review of fraud policies served as a fraud prevention technique or deterrent, resulting in few cases of unethical behaviour. Some banks have clear policies about how to handle grievances caused by unethical behaviour. Moses (International bank) notes that the bank has a clear procedure for handling

ethically uncomfortable situations for employees. Those that did not report recent unethical behaviour attributed this to the fact that people follow structures and procedures. Elijah (International bank) reported that his bank used these procedures to ensure discovery of unethical action, echoing Simon's view of ethics policies as a hard-line deterrent rather than a fuzzier cultural view. Paul (Local bank) also indicated that his bank took a zero-tolerance approach to unethical behaviour, suggesting that these banks have a much stronger view of the importance of ethics than some other organisations.

An important finding was that the relatively smaller banks did not report any marked incidences of unethical behaviour. This could be attributed to the fact that smaller banks may share common organisational culture and are more closely knit making it much more difficult for staff to carry out fraud undetected.

6.4.1.3 Reward Culture

This study looked into how banks seek to enforce deterrence in a positive way (Question 28 on interview schedule). Deterrence is often looked at as negative concept. However, there are ways that an organisation can positively deter its employees. Interviewees were asked how they enforced deterrence in a positive way.

A number of interviewees revealed that they provide rewards and incentives to staff as a means of positively deterring the occurrence of fraud. Caleb reported that there were varying incentives to prevent fraud and encourage its detection. Jacob indicated that whistle-blowers were rewarded, as were those that were not engaged in fraud. Other banks, mainly the international banks talked about various schemes and policies that are in place to encourage staff members to actively participate in fraud prevention. Moses' bank uses official recognition of those that assist in fraud prevention, while Joshua's bank uses a fraud hotline and spot awards as well as percentage-based awards for reporting fraud. A frequent theme was "speaking up", and this was frequently rewarded monetarily or with other recognition. Ruth indicated that her bank spelled out bonuses and salary increases available to those that comply with the code of conduct in the employment contract.

Monetary incentives were not the only approach taken. For example, Abraham indicated that his bank offered employees opportunities for education and training to increase commitment and reduce fraud. However, Gabriel indicated that recruitment and induction and training were basic elements in aligning people to the available incentives, and that incentives could not work on their own. Adam stated that a first line of defence was good pay, and that whistle-blowing and monetary awards were secondary. Solomon, conversely, indicated that good staff relationships were instrumental in encouraging staff to come forward and report fraud. Even in giving rewards Solomon mentioned that keeping good staff relations encouraged people to come forward and report fraud. Other than giving rewards, Thomas explained that his bank also encouraged staff members involved in fraud to speak up and in exchange receive a reduced punishment. Titus indicated that the identity of whistle-blowers was not disclosed and that they would be transferred for protection if necessary. Joseph's bank did not use monetary rewards at all, instead emphasizing organisational commitment and job security as incentives.

6.4.2 Structural and Institutional Issues

The study sought to identify structural and institutional issues that banks faced in the course of fighting fraud. Respondents were asked the following question (Question 29 on interview schedule): "In the process of fraud there are four main elements, namely: Prevention, detection, investigation and prosecution. Could you briefly discuss some of the challenges the organisation faces in these areas?"

6.4.2.1 Challenges in preventing fraud

Out of the 17 interviewees only 4 of them said that they hardly faced any challenges in preventing fraud. Others reported varied problems in attempting to prevent fraud. Ruth (Regional bank) said that preventing fraud was difficult where external actors were concerned as *"the persons sent to carry out fraudulent transactions may just be a third party. So the person you catch might not give you much information."* However, as revealed by Abraham (International bank) it is not only external factors that make fraud prevention a challenge but also cases that involve more than one bank raise inter-bank co-

operation issues. Often banks do not co-operate when it comes to sharing information. This makes it difficult prevent fraud spreading and affecting other banks. Adam (International bank) adds that there are co-operation problems when seeking vital inter-bank information on fraudsters. Nonetheless Moses (International bank) and Thomas (Regional bank) are of the opinion that success in prevention has to do with the people whose job it is to ensure fraud is minimized. Thomas states *"Procedures and controls are as good as the people who follow them. If people don't follow them and you have good measures then it is like you are doing nothing."* In other words fraud prevention is not only about having controls and systems in place, but it is also about the kind of personnel you are having who will enforce the rules and procedures. Moses went further:

"Prevention has to do with the controls we have put in place in our processes. These are as good as the people, the integrity of the people, who are manning them. In terms of enforcing prevention there are lapses because of a lack of enforcement of the controls on the part of the staff."(Moses - International Bank)

Paul (Local bank) commented that the changing or evolving nature of fraud presents a challenge and the staff must remain on guard, aware, alert and educated consistently in order to identify the new forms frauds take on. On challenges posed by prevention, Joseph (local) and David (Regional) held the view that some prevention challenges are due to management taking too long to make decisions on audit and other queries; meanwhile the fraud will continue.

6.4.2.2 Challenges in detecting fraud

Challenges in detecting fraud related to delays in obtaining and accessing necessary documentation (Adam and Solomon). Detecting of fraud is also slowed down by data going "missing", being destroyed or deleted (Moses and Thomas). Data was also not received in a timely fashion to facilitate detection of some fraud (Joshua and David). It is hard to follow up and detect fraud in the absence of crucial information that may be held by customers (Caleb, Jacob and Ruth)

6.4.2.3 Challenges in investigating fraud

Challenges in investigating fraud yielded varied responses from the interviewees. One of the challenges faced by the banks was the fact that employees were reluctant to implicate their colleagues who are involved in fraud and this frustrated the investigations. There was also lack of co-operation from the police, management and other banks. The police and prosecutors lacked skills in carrying out investigations and cases took a long time with the police. In some cases the costs of investigating the fraud were prohibitive. During the process of investigating cases the banks face resistance by staff through the union that can shield the perpetrator. Other challenges included receiving threats from the fraudsters and fraudsters holding back information.

6.4.2.4 Challenges in prosecuting fraud

The aspect of challenges that evoked most response from the interviewees was that of prosecution. Banks indicated that there were only weak provisions for fraud detection and prosecution available, that the legal basis for fraud prosecution was inadequate, that prosecutorial, legal and law enforcement knowledge of fraud was lacking, and that the legal process was difficult and extended. These factors often moderated against the use of the court system in dealing with fraud. The study raised some legal issues in respect to prosecution and legal enforcement that are discussed below. Themes cover legal problems regarding the length of time it takes to prosecute fraud, the high acquittal rate, issues surrounding the police force and the justice system. More about issues arising from prosecution are covered in Section 6.4.2.4.1 – Section 6.4.2.4.5

6.4.2.4.1 Prosecution

Prosecution was one of the major challenges that respondents indicated they faced in fraud prevention. Some major issues included prosecution length and a high rate of acquittals.

Some interviewees talked about the long period of time they had to wait for a case that was before the court to be concluded. Hence many cases remain unresolved for many years. In the process of the delays some witnesses relocate, material evidence is lost,

fraudsters bribe their way out and people lose interest in the case. Ruth (Regional bank), Adam (A National bank), and Joshua (International bank) mentioned the length of prosecution, indicating a minimum time of three months and as many as ten court visits for a prosecution.

Problems with prosecution ran deeper than just length. Caleb (Local bank) indicated some cases had been on-going for more than seven years, stating that courts do not schedule cases in advance, but instead summon all witnesses at once for as many as 100 cases, causing witnesses to miss court appearances. Solomon (Local bank) suggested cases could take eight years, and that further problems included prosecutorial and judicial independence, lawyers seeking adjournments and delays, and police transfers standing in the way of case completion. David (Regional bank) indicated that the judiciary was backlogged; both Solomon and David suggested that witnesses frequently disappeared or were compromised during this time. The length of time taken for prosecutions is both costly and reduces the deterrent power of criminal prosecution, ultimately harming banks.

A judicial issue raised through the interviews was the high rate of case acquittals. Some interviewees explained how they have flagged up this issue within the industry. This high rate of acquittals frustrates the efforts made by banks in arresting and prosecuting fraudsters. At the same time fraudsters remain undeterred as they know they can buy their way out of the legal system. Moses (International bank) asserts a 95% acquittal rate, mostly due to police and prosecutor failure to understand evidence.

Corruption in the judicial system was also cited as a challenge which eventually leads to fraudsters being acquitted. Titus (A National bank) indicates that *"fraudsters have connections in the judicial system and end up getting an acquittal."* David (Regional bank) suggests most acquittals are due to technicalities. He states that this has been raised at the industry and police commissioner level, but that corruption is still rampant. It is clear that the judicial system needs to be strengthened to reduce the effects of corruption.

6.4.2.4.2 The legal system

The legal system in general, including police, prosecutors, and judges, causes issues in effective prosecution. Abraham indicates that a lot of time is wasted trying to deal with the system. Joseph states that managers must rely on legal advisors, and that prosecution is inconvenient and postponements are common. Joshua, Titus and Moses indicated that prosecutors and investigators lacked skills and knowledge to effectively prosecute crimes. Titus and Simon suggested that judges and magistrates often misunderstood crimes as well. Moses suggested that along with a lack of skill, prosecutors had no desire to understand the problems encountered. An apparent lack of equipment, facilities and expertise is a further challenge. Solomon indicated there were no forensic laboratories, document examiners, or other facilities for effective investigation in most cases, as well as a lack of IT knowledge and expertise.

6.4.2.4.3 Cost Versus Benefit

Other than the challenges raised by the legal system the legal fees at times do not compensate for time and money lost. Joseph indicated that for small amounts, too much time and costs were incurred for prosecution to be worthwhile. Caleb agreed with this, especially since monetary recovery was rare. The banks do not find it beneficial to take legal action where the cost of prosecution is greater than the amount recoverable from the fraud. As prosecution is a measure of deterrence, we can infer that striking a trade-off between deterring fraud and the costs associated with deterring fraud is an issue in fraud risk management.

6.4.2.4.4 Frequent transfer and slackness of the police force

The regular transfer of police staff who are investigating and prosecuting cases within the central bank fraud unit has greatly reduced the speed at which some of the cases are concluded. This further exacerbates the situation seen in Section 6.4.2.4.1, where length of prosecution makes police transfers more likely. Solomon (Local bank) indicated one case where they had a police officer working on a case where they were able to provide direct information about the identity of the perpetrator; however, his replacement was not as passionate and the case was dropped. Jacob cited a lack of cooperation from the police,

especially a failure to take a statement needed to proceed with a case. Elijah (International bank) cited multiple cases being dismissed for unprofessional investigations, and noted that this served as a significant reason for developing internal procedures. An overall sense of apathy and unprofessionalism on the part of police prevents completion of investigations.

Moses indicated that passing a case to external investigators often resulted in a less effective investigation, since house investigators are generally well-trained compared to police. He stated:
"Most of the police are in a hurry and not ready to sit down with the internal investigators to understand a case and the process. They don't see the need why they should understand the whole process first before they look at what offence has been committed. This leads to the case evidence not being properly compiled."(International bank)

One of the biggest concerns to the banking industry is the high turnover of police personnel at the Banking Fraud Unit (which falls under the Central Bank, Police Unit) charged with the responsibility of investigating banking fraud cases. Moses notes that the unit has a high turnover rate. The department has frequent overhauls (three to six months), and experienced staff is routinely swapped for inexperienced staff. The investigative staffs also fail to listen to input from internal investigators. David confirms this situation, and also states that the department is understaffed. The researcher confirmed the problem of frequent transfers and inexperience. On visiting the Banking Fraud Unit, all the personnel were recently transferred after just 3 months in office. Moses suggests that there is some form of nepotism where police officers are appointed through connections (family or otherwise) implying that there are problems within the system.

6.4.2.4.5 Weak legal enforcement and poor industry co-operation
Investigating fraud at times requires the assistance of a third party, which in the case of this study is either another bank or a law enforcement institution. This study revealed that

there is little co-ordination between banks. And at the same time the police are not quick with assisting in bringing culprits to book. Adam observed that often frauds were cross-bank, but investigation began in another bank, and that investigation was difficult without involving other banks, the court and police, and the central bank. However, this is hampered by a weak cooperation in the industry. This is particularly true because of the high cheque fraud load. Caleb cites difficulty getting information from other banks, like CCTV tapes. This offers an opportunity for improvement in the industry.

In concluding the findings in this section certain issues stand out: Court cases are taking too long to resolve; the rate of acquittals is high; the legal and law enforcement system, including police investigators, prosecutors, and courts, are not very effective; and industry co-operation is weak. Arising from this are questions regarding how banks can deal with fraud given the deficiencies in the legal institution. How can problems encountered with the legal and law enforcement systems be tackled? Why is the banking industry not working co-operatively to fight fraud formally? These issues will be discussed further in the next chapter.

6.4.3 Cultural Issues

Respondents were asked "What cultural and social factors contribute to unethical behaviour in your organisation?" (Question 24 on interview schedule)

The main cultural issue that emerged was the divide on the issue of tribal influences as a contributing element in fraud. Among those who believe that fraud has nothing to do with tribal/community affiliations was Joseph, who said:

"There is a belief that certain communities are born thieves. I do not think it is true. It is just a culture that we propagate and try to justify that it is a part of culture."(Local bank)

Instead, he believed that this perception was a form of stereotyping, and that tribal affiliations were used as an excuse or scapegoat; instead, fraud happens all over, wherever people see motive and opportunity (indirectly referencing the Fraud Triangle).

Joshua opined that fraud occurred in both high-status and low-status people of different tribes or cultures, and was not confined to a certain culture. Simon shared similar sentiments as Joseph in saying that a thief is a thief and it has nothing to do with culture.
However, some respondents felt differently. Titus remarked, *"There could be some tribal and cultural elements though it is not a big issue. But there are tribes that need to be guarded carefully as they are very aggressive people."(A National bank)*
This seems to imply that there are some tribal overtones involved in the perception of fraud within the banking industry. Gabriel remarked that "*there are particular tribes that you never miss in a fraud trail," (Regional bank)* while Moses stated, "*most of the perpetrators or fraudsters come from specific regions of the country."(International bank)*

A number of social factors other than tribal affiliation were also discussed. Adam did indicate there was a certain age group (20s-30s) that were particularly involved in fraud. (This contradicts the findings of the quantitative study, which found that 31-40 was the most common age group, consistent with previous studies.) Caleb (Local bank) indicated that substance abuse and gambling were often involved, while Ruth (Regional bank) cited pressure to live beyond one's means as a major factor. Other respondents agreed with Ruth's observation.

Solomon explained his theory of "differential association" as an explanation of social factors contributing to fraud. Giving an example he said:
"…someone was working here and leaves on account of fraud and he still retains his friends… Probably he is now a full time fraudster. There are some people who have had a low integrity threshold and they have been recruited. There is also peer pressure, drinking, economic survival, poor role models – no one is condemning them about the way they have achieved their riches; or where people see fraud as a very intelligent exploit!"(Local bank)

It is worth noting that most participants seemed very guarded when answering this question. However, it seems it would be unwise to ignore socio-economic, and in particular, tribal considerations, when seeking to understand attitudes to fraud in Kenya.

6.4.4 Socioeconomic Issues

The socio-economic issues were identified from the same question as that asked in Section 6.6 above i.e. "What cultural and social factors contribute to unethical behaviour in your organisation?" (Question 24 on interview schedule)

In the course of the interviews interviewees explained some socio-economic issues that have led to the occurrence of fraud. One of these issues is unemployment and another economic constraint.

Adam implied that there was a direct link between unemployment, crime and fraud, and that much bank fraud was the follow-up to violent crime such as muggings. Others supporting a similar kind of view were Solomon, Thomas and David. Solomon (Local bank) cited a population explosion and lack of jobs as a factor in fraud, noting that it was difficult to control for this reason. Thomas cited unemployment and inflation as economic factors. However, according to David (Regional bank), some people have taken up fraud as a profession rather than as a desperation measure. However, from some of the fraud cases discussed with the interviewees some of the perpetrators were people in employment. Thus, these views must be considered critically, and are a cause for discussion later in Chapter 7.

Another socio-economic issue that surfaced from the interviewees was one that arises from the use of fairly recent banking technologies such as online and telephone banking. The socio-dynamics present an even greater risk to the customer – that of actual physical risk. Criminals in Kenya have been known to escort their victims to ATM machines to withdraw funds from their accounts; even holding their victim hostage for a number of days so that they can make daily withdrawals until the account is fully depleted of its funds. Telephone banking can therefore make the customer vulnerable to physical attack.

Solomon, talking about the risks that the customer faces with increased automation, voiced this concern but usually the risks lie with the account owner who e.g. fails to erase certain information about their transactions. This has been one factor in banks rejecting technologies that allow for this type of access. Respondents also expressed fear for their own safety as those that prosecute fraud. Adam indicated there was a potential threat to physical security.

6.4.5 Information Technology: Computer-based Crimes and New Challenges

Kenyan banks are yet to make significant forays into computer-based personal banking, according to respondents, maintaining these services primarily for elite customers. However, this has not prevented computer-based fraud become increasingly prevalent. Banks have also faced issues such as identity theft, which have challenged existing models of fraud detection and prevention. Respondents were asked two questions that related to the banks' susceptibility and vulnerability to fraud. Question 10 and 11 respectively asked: "Has the organisation had any fraud incident involving the misuse of computers/computer networks/online banking or organised criminal groups?" and "Has internet banking increased your banks vulnerability to fraud?" The responses are given in Sections 6.4.5.1 and 6.4.5.2

6.4.5.1 Susceptibility to computer related fraud and organised crime

The researcher asked whether the organisation had suffered any fraud incident involving the misuse of computers/computer networks/online banking or organised criminal groups.

The research revealed that a majority of the banks have not yet suffered Internet related frauds, even those occasioned by hackers. One of the main reasons that could explain this is that most banks have not yet moved into Internet banking. Those banks that have begun Internet banking have only rolled out the concept to a small group of bank customers, and this being still a privileged service; it is not open to all account holders. Currently the frauds suffered which relate to online or Internet banking is as a result of

customer negligence in securing their passwords and hence affording fraudsters the opportunity to exploit the lapse in security. The onus of keeping the account information safe and secure remains with the customer. Solomon and Moses both stated that customers had so far been the main weakness point for Internet-based fraud.

Banks are beginning to face the reality that they will need to offer Internet and phone banking. Adam stated that his bank recently launched an online service, which already was subject to hacking attacks. Joseph reported that so far there had been few problems with the bank's limited roll-out of Internet banking, but that they saw problems with identity theft as likely following a more comprehensive implementation.

Identity fraud is a growing problem in Kenya's banking industry. In the course of this research, it has become evident that fraudsters have access to facilities that enables them to produce fake passports, identification cards and even cloning credit and debit cards. With such falsified identity documents the fraudsters can gain access to customer accounts unlawfully withdrawing their money or they use the documents to open new accounts under false names. Paul suggests that proper scrutiny can prevent the use of these fraudulent documents. However, Solomon and Moses indicate that card skimming is increasingly common and facilitated by internal sources with inside information. Moses saw a conflict, in that the bank offers IT innovations to improve customer service, but these functions also increase the ability to defraud the bank. Solomon admitted that these IT-enabled frauds, frequently performed with insider help, were difficult to keep up with.

As mentioned in Section 6.2.1, collusion facilitates the leakage of customers' vital banking information enabling the fraudsters to clone debit and credit cards. Even as the banks strive to keep up with technology they face a challenge not only from external forces but from their own staff working with external collusion. Titus indicated that insiders, rather than external hackers, were responsible for manipulation of computer systems. David indicated that ex-staff were frequently involved in these frauds, having inside information and contacts that allow them access.

Other than incidents involving card fraud syndicates, where there could be a possible external organised link, the banks did not report any major problems of organised criminal activity. Joshua summarized this well when he stated that:
"We have not had an organised gang or hackers attack our system. Just amateurs using skimmed cards or employees trying to manipulate passwords to use the system to transfer funds or using wrong information."(International bank)

There was apparently difficulty identifying differences between ordinary fraud and organised crime. As Elijah said "*we had a series of fraud that were similar and I cannot rule out that those people were an organised group."(International bank)*
This uncertainty can be attributed to the complexity of organised crime and the difficulty involved in pinpointing it.

There are other issues that affect the fight against computer fraud in the banks. One such issue is system problems. The computer systems do not have built-in anti-fraud tool, leaving banks dependent on manual systems. In some international banks, even they use very fast transaction-monitoring systems. International banks also have access to systems developed outside Kenya. Modernizing systems will help banks curb frauds like card frauds. At the time of research, Kenyan debit cards used magnetic stripes rather than chip and pin, increasing the ease of card fraud and use of skimmed cards from other countries. How much is being done by the banks to make customers aware of information technology-related fraud and identity theft is an issue arising from this section.

6.4.5.2 Banks' increased vulnerability to fraud due to Internet banking

The interviewees were also asked whether Internet banking had increased their bank's vulnerability to fraud. As banks attempt to take on new computer technology they may invariably find themselves exposed to fraud due to increased vulnerability. Adam (A National bank) indicated that an increasing public profile due to online banking had increased fraud such as cheque fraud and fraudulent account opening. Paul (Local bank)

indicated that jurisdictional issues also were introduced with online banking, requiring increased cooperation between banks and institutions. (See Section 6.3.3.1)

Perceptions of exposure and vulnerability to fraud because of online banking vary depending on how much experience the bank has had. International and regional banks have had more experience, while local and national banks have had less exposure (with mainly corporate customers). However, the banks are well aware of the risks associated with online banking based on the experiences of other countries and the global trends. Titus (A National bank) and Gabriel (Regional bank) indicated that they are aware of risks from publications and other transmissions of experience. The general opinion is that online banking will soon become a serious risk.

At present most of the risk and vulnerability of online banking lies with the customer. However, increasing bank profiles will mean that banks will need to improve their security systems. Caleb (Local bank) stated that he was investigating what problems and risks his bank could expect from the introduction of online banking. However, banks are not put off by this, instead considering it as part of a cost-benefit analysis of increased business and commensurate increased risk. Responses indicate that banks are aware of the risks, are willing to face them and are preparing themselves to take these risks.

On the contrary as some banks reported that advancement in computer technology has in effect minimized fraud occurrences and limited it to internal problems. David (Regional bank) stated that online fraud was relatively simple to spot as compared to the complex collusions and accidental negligence associated with other frauds. However, other respondents did admit that card skimming by staff had occurred. However, banks do face higher losses from these frauds than traditional frauds, according to Solomon. Additionally, the lack of paper trail in computerized fraud systems makes problems for investigation.

We can therefore conclude that in spite of the risks attached to online banking, banks are beginning to provide these services to remain globally competitive. Perhaps the main

issue that arises here is how much of a risk banks are willing to take by embracing online banking as fraud management is also really about risk management.

6.5 Other Issues

There were a few issues from the research that are significant to discuss. One such issue is emerging fraud and international transactions. These are discussed below.

6.5.1 Emergent fraud and lack of proper legislation

The interviewees were asked if they were aware of certain frauds existing in other countries that could likely find their way into the Kenyan financial sector (Question 25 on interview schedule) and what measures were being put in place to combat such emerging fraud before they hit the industry (Question 26 on interview schedule).

There was a general feeling that Kenya has already been exposed to most of the frauds happening in the rest of the world; putting it in the words of Gabriel *"a majority of the frauds are here with us."* This view was supported by Simon, who stated that fraud was a globalized problem:

Any fraud which is committed in London or Johannesburg tomorrow morning it is in Nairobi. Because of the technological advancements we find that fraud now is almost the same anywhere. So there is no strange fraud that is prevalent in London and not in Nairobi…it's exactly the same."

Joseph argued that the prevalence of banking technology meant that Kenya's banking industry was interconnected to the global world of fraud as well. He noted that IT usage was a major point of fraud exposure. Adam and David confirmed that credit card and identity fraud were becoming increasingly prevalent. However, there was a feeling among respondents that Kenya had not yet seen the full force of technology-enabled fraud. Joel believed that Internet-based fraud was still emerging in the market, while other respondents, including Ruth and Titus, saw credit card fraud and card skimming as fraud that would become more prevalent in future. Elijah sees Africa as the obvious next point for targeting of credit card fraud. Caleb saw an opportunity for improvement in

adoption of the chip and pin system, indicating that banks needed to adopt the system by 2010 or they would be liable for fraudulent actions, indicating a regulatory change.

The responses above indicate that banks are now increasingly encountering credit and debit card fraud. However, in Kenya the legal environment that banks operate in has made it difficult for banks to prosecute card frauds. The bankers noted that prosecution of card skimmers is difficult as there is no credit card legislation in Kenya. Moses explained the present situation this way:

"The Attorney General is in the process of drafting Credit Card Legislation. They have borrowed heavily from the South African and UK legislation. They are putting it together. The legislation has still not yet reached the Parliament but it is at an advanced stage because I know we are actively involved including other stakeholders. But that has been our major challenge…..we still recover this crime but we can't successfully prosecute because of lack of legislation."(International bank)

Without legislation the banks have no teeth to fight this type of fraud. Approving Government legislature often takes multiple levels and in the process valuable time is consumed. This is a great setback for the banking industry as it continues to suffer this fraud relentlessly. The fraudsters are aware that they can get away with it and will therefore keep exploiting the loophole created by lack of legislature.

In light of the awareness that card fraud is a present and still emerging fraud, what are banks doing to prepare themselves? What progress has there been in getting the Credit Card Legislature passed and in advancing to "Pin and Chip" system? The next chapter will explore these issues as well as the possible advantages the legislature and "Pin and Chip" system will bring to the banking industry in terms of fighting fraud.

6.5.2 Domestic and international transactions

Over the past few decades globalization has changed the face of many industries, especially the banking industry. With globalization new opportunities and benefits have been brought to the banking industry. However, it has also brought some challenges.

One of the issues resulting from globalization is that of jurisdiction in investigating fraud. This issue arises as an offshoot from Question 3 (Who are the perpetrators and how was the fraud detected) where some cases involved fraud committed across the borders and their impact. One of the interviewees, Adam (A National bank) recounted a fraud incidence where a series of cheques had been stolen from a foreign embassy in a neighbouring country. In the process of this case being investigated it was discovered that one of the cheques (the fraudulent cheque passed on by the perpetrator to our customer) had gone through. The case of the stolen cheques had already been reported to the German police, but the paying bank was not aware. It is only in the process of the investigation that they realized one of the cheques had come through. This created a great deal of confusion regarding jurisdiction. At the time of reporting, the case had gone on for three years, with Adam's bank being forced to take the financial hit for the fraud. However, there was no way for them to detect or monitor this type of fraud.

Different rules operate in different areas of jurisdiction. This raises the issue about how to effectively carry out fraud management in cases that transcend borders. Adam reports that even simple issues like whether a cheque can be paid is confusing. Paul (Local bank) discussed a case involving a fake international cheque, indicating that local fraudsters capitalised on confusion regarding international cheques to create fake documents. Paul reflected:

"I would imagine a situation whereby some instructions purportedly come from Europe and here I am in Africa, in the middle of Africa and I do not know whether these instructions are genuine. So it comes with its new challenges and we need to work harder to counter them."

With increased globalization competition is bound to reach dizzy heights. Increase in competition brings with it a degree of fraud risk. Can the banks effectively tackle international fraud and is international fraud a big threat to fraud security in the industry? This issue is addressed in Chapter 7.

6.5.3 Reducing Fraud

A general question was asked (Question 29) concerning what the respondents thought could be done to reduce fraud in the banking industry. A summary of the responses includes: the banking industry in Kenya needs to learn/adopt from the experiences of developed countries; fraud training needs to be extended to the customers as they are the main detectors of fraud; internal control systems need to be enhanced to deter fraud; the banks also need to keep abreast of the fraudster – be one step ahead;

6.6 Reflections on research questions and conceptual framework

This chapter has discussed a number of themes that relate to the first three of the following four research questions:

1. What are the characteristics of fraud in the Kenyan banking industry?
2. What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?
3. How do banks approach fraud management?
4. Are there differences between the approaches to fraud management adopted by Kenyan and international banks?

Considering Research Question 1 a few characteristics of fraud have come out of this qualitative study. The theft of cash, passing of fraudulent cheques and identity fraud are among the main types of fraud reported, agreeing with the findings of the quantitative study. Most of the frauds are reported to the police but recovery of fraudulent funds is low. A typical fraud would be in the order of about is KES 5,000,000.

The findings of the qualitative study reveal some characteristics of those who perpetrate fraud in the banking industry as pursued in Research Question 2. Based on interviewees' fraud experiences, fraud is mainly perpetrated through collusion of internal and/or external perpetrators. Like the quantitative study this study has also identified that the average age of the perpetrators lies in the age bracket of 31-45 years age and perpetrators are mostly male but with a significant number of female participation reported. Internal

perpetrators predominantly held positions of cashiers, tellers and clerks and had on average served for a short period of time. Motivations again point to financial pressure, opportunity and peer pressure while fraud opportunities are provided through poor internal controls, lack of segregation of duties and lax supervisory control.

Research Question 3 on how banks manage fraud was the main focus of this study. The study shows that there is room for improving fraud management. Internal control systems require tightening, strengthening and enforcement. The recruitment for screening procedures needs to be managed better to reduce the instance of possibly hiring people with questionable backgrounds. Fraud prevention and detection should be improved by training customers as a majority of fraud is detected by them. Fraud budgets should be clearly defined and planned for. Efforts towards creating industry co-operation should be considered so that banks can share information and work together to fight and reduce fraud incidences. Competition for customers and profit margins needs to be considered in context of the fraud risk that this competition generates. There are ethical issues that have implications for the industry and the banks should strive to establish best practices. Structural and institutional issues pose a great challenge in the management of fraud with the main challenges being in the prevention and prosecution of fraud. Changes and improvements in the legal and justice systems and institutions appear to be the way forward to better and more effective fraud management. Cultural and socio-economic environments are broader issues that have an important bearing on fraud management. Understanding these issues can help organizations tackle fraud better. Finally as banks begin to increasingly embrace information technology (IT) precautions should be taken to bolster internal IT defenses including using appropriate software and technology. Proper fraud risk management should be contemplated so as to determine bank susceptibility and vulnerability to fraud.

The qualitative study has provided some further and more in-depth answers to the research questions as discussed above. The identification of emerging frauds serves as a window to establishing future control measures.

This chapter has been structured in such a way that the conceptual framework can be identified. Section 6.2 captures the perpetrator and Fraud Triangle, which is the central part of the conceptual framework. Internal factors of the conceptual framework are discussed in Section 6.3 while Sections 6.4 and 6.5 relate to the external factors of the conceptual framework, completing it.

6.7 Summary

This chapter has highlighted the main findings that have emerged from the field interviews with respondents from the banks. Main themes were based on the perpetrator – collusion and the fraud triangle. Other themes were based on the internal factors of the conceptual framework and included internal control systems, fraud prevention and detection and deterrence. Respondents report that customers, rather than internal controls, uncover most fraud.

One major theme is relationships between banks and customers, which may be cooperative or competitive. KBA involvement indicates cooperation, but banks continue to compete for customers, which has impeded joint fraud detection and prevention efforts. However, perhaps the biggest barrier to effective fraud prevention are the external factors that are presented in the form of bank ethics, cultural, socio-economic, information technology, legal, structural and institutional framework that banks must work with. Legal systems are especially inadequate to deal with fraud and are inefficient in their dealings, leading to a situation in which the institutions actually impede, rather than promote, effective fraud prevention. Furthermore, banks now find themselves dealing with challenges such as computer-based fraud and identity theft, which their existing fraud mechanisms are not designed to handle. These themes will be developed further in Chapter 7, which also integrates the findings of the qualitative and quantitative research with the existing literature.

Chapter 7
Discussion

7.1 Introduction

The aim of this chapter is to integrate the qualitative and quantitative findings of this research with the existing literature in order to understand fraud in the Kenyan banking industry. Previously, the nature and characteristics of fraud in the Kenyan banking industry and its ability to prevent and detect fraud has been discussed, in line with the research questions associated with this research:

1. What are the characteristics of fraud in the Kenyan banking industry?
2. What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?
3. How do banks approach fraud management?
4. Are there differences between the approaches to fraud management adopted by Kenyan and international banks?

The qualitative and quantitative findings of this research have identified a number of different trends and factors that can be compared to existing research and analysed together in order to draw conclusions about how the banks are handling the issue of fraud. The findings conflict in some areas, although not in others, and in some cases do not support the existing state of the literature. This chapter summarises findings from the qualitative findings (Section 7.2), discusses major themes and issues and relates them to literature (Section 7.3), and integrates qualitative and quantitative findings (Section 7.4). Further points of discussion include differences between international and other banks (Section 7.5); relation of findings to theories of fraud (Sections 7.6 and 7.7) and discusses the implications of these findings (Sections 7.8 and 7.9).

7.2 Overview of Qualitative Findings

A brief summary of qualitative findings is provided below. These findings are detailed in Chapter 6 (Qualitative Findings). Key themes that were identified in the qualitative interviews included: collusion and internal controls; cooperation and competition between banks; customers; legal, structural, socio-economic, cultural, technology and other external factors. These findings primarily referred to Research Question 3 ("How do banks approach fraud management") although they also touch on Question 1 ("What are the characteristics of fraud in the Kenyan banking industry) and Research Question 2 ("What are the perceived characteristics of those that perpetrate fraud?")

Collusion between perpetrators was both pervasive and difficult to detect. Internal controls were seen as the main way to fight fraud, but were not necessarily successful. Banks do share information about fraud, which is an improvement on previous practices. However, participation in the KBA is uneven, which could limit its potential usefulness. Customers are a source of major competition between banks, and although there are safeguards against known fraudulent customers in place they are often circumvented. However, customers are also important in fraud detection as they are a main contributor in uncovering fraudulent activities happening in their bank accounts. Socioeconomic conditions including high unemployment rates and organised crime are seen as major factors in bank fraud. International transactions are also a major source of fraud.

Banks reported complacency and failure to follow protocols when hiring new employees, which increased the chance of fraud. Banks also reported differences in the amount of money available to fight fraud; banks had different attitudes toward fraud budgets depending on their overall views of fraud. One area Kenyan banks did not face a significant challenge as yet is the case of internet banking fraud, which is due to selective practices adopted by the banks as to the clientele that can access online banking. However, identity theft and debit and credit card skimming were common. Banks are currently in the process of modernizing their computerized fraud detection systems, and

some of these systems remain manual. Some banks do use a code of ethics, but this is not consistent and the view on whether or not this is effective varies.

One of the most significant issues that have emerged from the research is the problem posed by the legal system. Lengthy prosecutions make legal remedies very costly for the banks, and there is a high rate of acquittal for cases brought to criminal trial. There is overall a lack of expertise in the judicial system regarding bank fraud, and some concerns about corruption. Poorly trained police officers mean that many cases cannot be prosecuted successfully, and there is overall a lack of stability, equipment, training, and facilities, as well as a lack of legal structures and laws to address some types of fraud. Many banks choose to avoid prosecution because cost-benefit analysis shows that it is more trouble than it is worth.

7.3 Discussion on Qualitative findings

While the quantitative findings of the study were effective in describing fraud, the qualitative findings provided significantly more insight into the issues the banks considered important. These findings also identified some differences in the Kenyan banking system as compared to the general banking system.

The conceptual framework discussed in Chapter 3 (Section 3.10) was constructed around three broad components: The individual perpetrator was represented by the Fraud Triangle, the immediate internal environment within the banking industry and the external environment surrounding the banking industry.

The main issues that emerged from this research can be arranged along four thematic lines identified; including relationships between banks, employees and fraud detection, structural and institutional issues, and computer-based crimes and emergent challenges. These themes have been arranged based on the conceptual framework.

7.3.1 The Perpetrator

The qualitative research reflected a number of different relationships between banks, employees and fraud detection that provide keys to the development of a basic theme

regarding the individual or employee as a perpetrator (Section 7.3.1.1) and collusion (Section 7.3.1.2). Section 7.3.1 focuses on Research Question 2. It also addresses the central aspect of the conceptual framework (the individual perpetrator and insider collusion) in Chapter 3, Section 3.10.

7.3.1.1 The Individual Perpetrator

The conceptual framework focuses on the individual using the classical model of the Fraud Triangle (Cressey, 1973; Wells, 2005). In the fraud triangle, the pressure to commit fraud begins with a non-shareable financial burden, which provides the motivation to commit fraud. The individual must also have the opportunity (including access and skill) to commit the fraud, combined with the ability to rationalize the crime in accordance with ethics, need, or some other factor. This rationalization is then discarded following the fraud, though it may re-emerge on the fraudster being challenged (Cressey, 1973; Wells, 2005).

Cressey (1973) identifies six main reasons for fraud, and the findings of this research were consistent with some of these reasons. Most of the reasons found in the qualitative and quantitative studies found that status-gaining problems were the main motivations used, especially overconsumption. However, there were no significant statements regarding isolation and employee-employer relations. Violations of obligations like gambling or drugs were not apparent which is in contrast to Cressey's findings. Personal failures also were not apparent. However, family issues like the need to pay school fees did emerge. This indicates some consistency with the fraud triangle's motivations, and importantly did not indicate any findings that were outside this model. However, the use of bank representatives rather than perpetrator information for this question could result in some degree of bias in the findings.

The second leg of the triangle refers to opportunity. The study revealed that those who perpetrated the fraud had ready or easy access to the funds. Most of the internal perpetrators used their positions – cashiers, tellers, and accountants - for committing fraud. The majority of frauds perpetrated, according to participants, were small-scale

frauds (with an average value of around US$1,500 in total) that were based on cheque and cash misappropriation or theft, manipulation of customer accounts, or other means that were readily available to the majority of bank workers. This is consistent with the need for opportunity (Cressey, 1973; Wells, 2005). Only one case could potentially represent a much larger-scale fraud. Cash and cheque handling controls could reduce this opportunity. It is possible that, given the relatively small sums (which are large in relation to salaries), that feeling underpaid could be an unstated motivating factor. This would also be consistent with Cressey's model.

Finally there is the issue of rationalization. One consistent rationalization was that everyone was doing it. This speaks to a rationalization in which the external environment of fraud is used as justification for the fraud, and which creates confusion between the external environment and internal ethical norms (Aguilar et al., 2000; Cressey, 1973). Thus, the external environment poses a challenge and it is one area where it is possible that the banks could influence fraud.

One factor that is not discussed in the Fraud Triangle is collusion, or conspiracy between two or more parties in order to commit fraud (Breuer, 2006). The quantitative and qualitative studies carried out in this research both revealed that there was a high incidence of collusion among and across internal and external parties. Collusion is known to occur between workers at the same level, at different levels, and internal and external parties (Breuer, 2006; Canhoto & Backhouse, 2007). The most common use for collusion in cases studied here is to overcome gaps in opportunity. For example, an individual with high technical skill but no access to cash stores may collude with someone with limited technical skill but increased cash access in order to perpetrate a fraud, or a customer may collude with a bank teller in order to receive cash (Canhoto & Backhouse, 2007). The current study indicates that internal collusion was mainly between junior employees and either supervisors (middle level managers) or senior managers, confirming the necessity of persons at different levels of authority to collude to provide an impetus for fraud. External collusion with customers, suppliers and even ex-employees was identified in this study. Each party played a significant role based on their position or access to facilities

required for fraud to be committed. The development of collusion is likely not included in the Fraud Triangle because it is developed as an individual model of crime.

Based on the findings in this study concerning collusion the researcher suggests a theoretical process chart that describes the way in which an individual may choose to commit fraud. This process chart demonstrates the individual characteristics that must be in place in order to allow for the commission of fraud within the banking industry in Kenya. This model can be used to examine the individual characteristics of the fraud and is shown in Figure 7.1. The problem of collusion is discussed in Section 7.3.1.2, as it has a strong influence on banking outcomes.

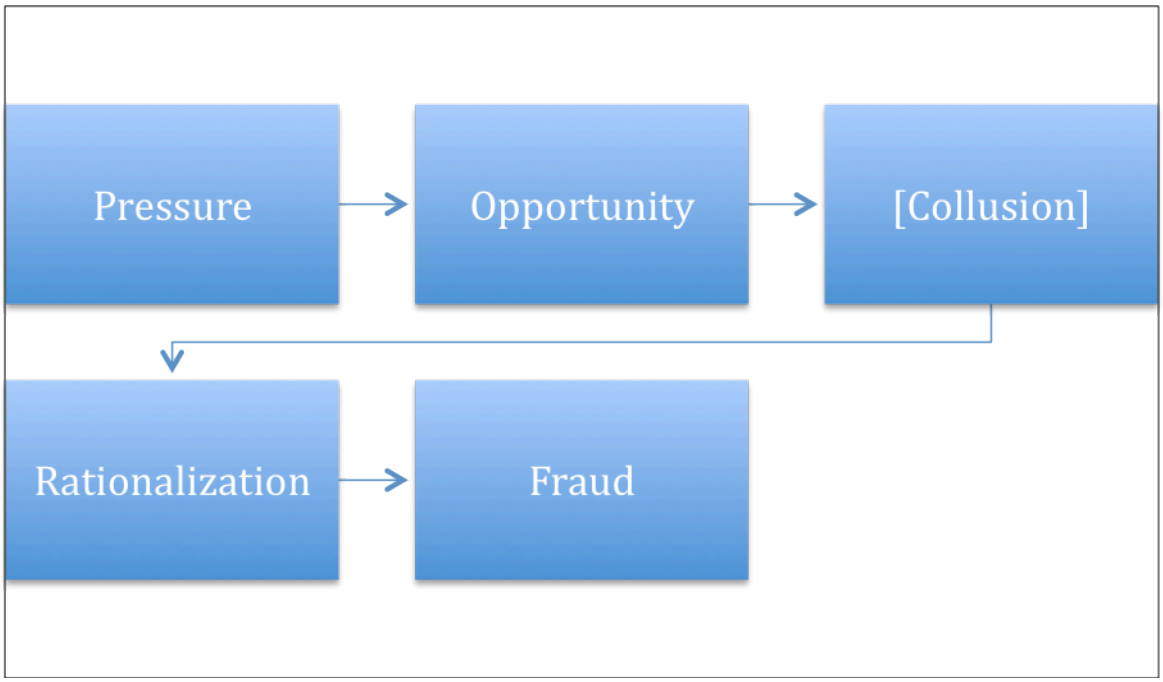


Figure 7.1: The process of committing fraud

7.3.1.2 Insider Collusion

Insider collusion was cited as the major source of fraud in the majority of fraud cases outlined in the surveys as well as the interviews. Almost all frauds reported involved at least one insider, while some frauds involved two or more. Collusion with outsiders was also reported.

These findings agree with recent reports which appeared in the Kenyan press (Okwembah, 2010) that claim that bank employees colluding with fraudsters had silently stolen KES2.4 billion Kenyan banks between January 2009 and July 2010. The Central Bank of Kenya statistics showed that KES 1.6 billion was stolen through collusion in 2010 (Okwembah, 2010). Okwembah (2010) suggests that banks are actually underreporting losses to protect their reputations, meaning that this is an underestimate. However, there are cases filed weekly at the High Court against employees of banks, indicating the degree of the problem (Okwembah, 2010).

The same source adds further that the figure of KES 2.4 billion is estimated to be much lower than what has actually been stolen as most banks remain silent to protect their reputations and to avoid bad publicity. However, this silence has not suppressed the number of fraud and theft cases that are filed by banks at the High Court, almost on a weekly basis, involving bank employees (Okwembah, 2010) which can imply that banks may be attempting to put some faith in the legal system. According to a confidential police report highlighted in the press, fraud through employee collusion is on the increase (Banking Fraud Report Shocker, 2010), lending support to the findings of the current research.

Insider collusion can be particularly difficult to deal with, especially given that insiders understand the fraud prevention methods in use and may be able to determine ways to avoid them. The banks reported using a number of different methods and internal controls for reducing the potential for insider collusion, including separation of duties, job rotation, internal audits, screening and recruitment controls and other systems controls. The issue of internal controls is pursued in the next section 7.3.2

7.3.2 Internal Environment factors – Banks and Industry

Another main component of the conceptual framework considers the internal bank and industry factors. One of these factors arises from the theme on internal controls. As discussed in the previous section internal controls can be used to reduce fraud and collusion. Another theme that emerged in the qualitative research was the tension

between cooperation and competition in the banking industry, reflecting an internal environmental characteristic.

The industry environment figures in eclectic models of fraud, which posits that weakness in industry groups and regulation is a determining factor in the prevalence of fraud (Riahi-Belkaoui & Picur, 2000). In particular, this industry weakness is reflected in the use of strong external assurances regarding the treatment of fraud, combined with internal disorganisation and lack of focus on changing institutions and priorities (Riahi-Belkaoui & Picur, 2000). There are several factors that can be identified at the bank and industry level, including internal controls, sharing information and competing for customers and customer fraud awareness. Research Question 3 is the main question addressed here ("How do banks approach fraud management").

7.3.2.1 Internal Controls

By resorting to the separation of responsibilities the banks are effectively breaking the fraud triangle by denying the potential fraudster the opportunity required to engage in fraud. Separation of duties acts as a safeguard or cushion against fraud and enhances security for the banks by limiting the amount of control a given individual has over any one area (Stewart, Tittle & Chappel, 2009). This was consistent with the bank's use of separation of duties. Findings also indicated that the bank used job rotation, including occasional short-term rotations to other regions, as a control mechanism. This had the effect of both breaking up existing collusion and providing opportunity for oversight from other employees. Job rotations are known to be one of the most effective means of fraud control, lowering loss to fraud by 61%, although they are not frequently used (ACFE, 2008). However, the organisations did not commonly use surprise audits, another internal control that is known to be effective, lowering median loss to fraud by 66% (ACFE, 2008). This provides strong support for the use of job rotation and indicates that more banks should consider the use of surprise audits as well. The case of K-Rep Bank illustrates the effectiveness of job rotation and surprise audits, along with other approaches (Campion, 2000, cited in Ledgerwood & White, 2006). By carrying out regular and sometimes unscheduled audits causes the employee to be weary that they are

being checked on. Auditing therefore serves as a deterrent (AICPA, 2012). In the current economic environment there is a greater demand for internal controls to work effectively. Like the USA and other countries that are leading the way in reinforcing the role of auditing in fraud prevention and detection, the banking industry in Kenya can benefit by learning from best practice. Even though Kenya's banking industry has not been largely affected by the recent global financial and banking crisis they can learn some lessons from the experiences of countries that are currently undergoing such crisis.

A notable weakness in the internal controls highlighted through the interviews related to staff screening procedures. Hiring the right employees is one of the first steps in preventing fraud. As already highlighted in the literature review appropriate background checks are essential and cover an individuals' educational and professional credentials, criminal record, history of employment, media and credit checks as well as honesty/integrity testing (Brody, 2010). However, this was an area of apparent weakness in the study. In some cases banks have hired employees that have been known or later discovered to have had a fraud history, and who have gone on to commit fraud. Furthermore, background checks are not fully effective, and honesty and integrity testing are recommended (Brody, 2010). None of the responses indicated banks used this method. Low personal integrity was revealed to be a problem, agreeing with Albrecht's (1984) fraud scale, which indicated that situational pressures, perceived opportunity, and low personal integrity are likely to lead to fraud. This further emphasizes the need for honesty and integrity testing (Brody, 2010).

Background checks and references were seen as methods to reduce collusion, but there were serious problems, such as not receiving referral letters and circumventing policy. Banks that simply dismiss employees accused of fraud exacerbate the problem. These measures are simply ineffective against fraud involving collusion, either internal or potentially through organised crime.

The problem of recruitment has been suggested in a confidential police report from the Banking Fraud Investigation Department recently released to the press (Bank Fraud

Report Shocker, 2010). This report questions recruitment criteria, indicating that most bank frauds involve bank employees, and that there was a strong link between recruitment practices and fraud. However, reference checks from credible sources are difficult to come by in Kenya, due to lack of organised criminal databases and other centralised systems. In Kenya the "Certificate of Good Conduct" is taken as proof. However, this system is vulnerable to corruption, making it less reliable. Even in cases where negative references are provided, they may be overlooked by recruiting officers, resulting in fraud.

Insider threat is a common problem in banking. Insiders have easy access to systems and have knowledge and understanding of how systems work. They can collude to defraud the bank activities (Brancik, 2007; Adams, 2010). This indicates that this is an issue that has been identified in other banking contexts and so should be considered seriously.

Responses relied on technical controls to detect and prevent fraud. However, these seemed to be mostly ineffective, with customers and personnel noticing most fraud. This is consistent with previous research, which has indicated that only around one third of complex fraud is detected by technical controls (Goode & Lacey, 2010). This does not make technical controls unnecessary, but instead indicates that they cannot be relied on. In particular, they are good at identifying isolated instances of fraud.

However, one bank suffered a loss of around US$1,200,000 as the result of a single complex fraud. Given that fraud detection mechanisms are generally aligned to detection of fraud at only a single level, the use of multiple methods of fraud detection is best for the organisation (Goode & Lacey, 2010). However, technical controls alone are not enough to detect fraud. Banks need to control corporate culture and personnel to limit insider opportunities. Given that part of the opportunity to commit fraud is having an understanding of internal controls and how to circumvent them, this is consistent with findings regarding this area of concern (Cressey, 1973; Wells, 2005).

Another issue is the corporate culture. The survey results indicated that a large number of respondents believed that fraudsters committed fraud because they saw others getting away with it. The interviews revealed more issues with the corporate culture that could affect how the organisation encountered fraud. For example, there was an indication that banks would simply dismiss those found to be conducting a fraud rather than prosecute, because of the associated financial and non-financial costs, and that they would often hire without waiting for references due to the length of time it took reference letters to reach the organization. These issues speak to organizational cultures where the issue of fraud is not considered to be highly important, and where other concerns, such as cost or expedience, take precedence. However, if the press report (Okwembah, 2010) mentioned earlier in this section is considered then perhaps there could be a perceptual gap about prosecution or a change in the way banks are handling prosecution of fraudsters.

7.3.2.2 The Kenya Bankers Association (KBA) and information sharing on fraud

Sharing information is one of the fundamental keys to prevention of fraud, because of the ability to reduce exposure to fraud (Barth et al., 2008). A major force for information sharing in the industry is the Kenya Bankers Association (KBA), but the KBA can only be said to be partially successful.

The KBA has been effective at standardisation and modernisation of the banking system in the past, such as implementation of the direct debit payment scheme (Central Bank of Kenya, 2003). The organisation is also currently undertaking some initiatives such as development of a fraudulent activity database, according to respondents. Another information sharing project is the Kenya Credit Information Sharing Initiative was created in 2009 as a project within the KBA leading to implementation of a credit information sharing mechanism in Kenya, which will allow banks to provide information to a credit reference bureau (Kenya Credit Information Sharing Initiative, 2010; Mwanza, 2010). This was enabled by the Banking (Credit Bureau) Regulations of 2008, discussed in Chapter 3. The ability to share credit information will be a step in the right direction to alleviating the problem of adverse selection and information asymmetries that has

previously been a source of bank failures in Kenya. This could also provide a template for other information sharing projects.

However, there were some problems with cooperation in this area. Some of the bank respondents indicated that their organisation often felt cut off or marginalised by the KBA, which they saw as prioritising the demands and input of larger banks. In the past and even in the present, most banks are reluctant to share information enabling fraudsters to operate within their systems undetected. A study by Waweru and Kalani (2009) on Kenyan banks found that information sharing among the banks concerning creditworthiness of borrowers was poor, as was the use of credit reference bureaus. This supports the findings of this study regarding information sharing. However, this attitude may be changing, as respondents believe that the sharing of information will deter fraudsters. This finding has been strengthened by recent reports appearing in the press (Okwembah, 2010) echoing similar sentiments within the banking industry. However, the actual level of information sharing is still relatively low, due to fear of negative publicity and loss of competitive advantage.

The absence of a common database for banks has facilitated identity fraud in the banking industry. There is some industrial discussion about centralising identities in a national database (Ndungu and Etemesi, 2010). This research does support the need for this service. However, creating a national database raises issues of ownership, security of data, access, individual rights, management, financial capacity, and human resources (UNDP, n.d). It is unlikely to be an immediate fix.

To achieve the initiatives mentioned in the paragraphs above the KBA has worked closely and deliberated with the Central Bank of Kenya, the Ministry of Finance and the office of the Attorney General. Given this, the KBA and its members should consider how the KBA can be modified to be a positive force in the development of the banking industry's approach to fraud prevention and detection. However for this modification to be effected will depend on whether the KBA is adequately resourced in terms of funding,

trained personnel, technical staff etc. Fraud is a global phenomenon and no one entity or body can tackle it alone. Hence a concerted effort is required from different entities.

7.3.2.3 Customer Fraud Awareness and competition

One of the major findings of the study was that the majority of frauds were found by customers whose accounts were affected. This suggests that inadequate or ineffective internal controls are being used. However, it also suggests that there is an opportunity for improvement in broadening fraud detection capacity in banking institutions. There were only a few banks that indicated routinely using fraud awareness or education for their customers. There are several potential reasons that banks may not want to support or engage in customer education regarding fraud, which are discussed in greater detail below. However, this does not mean that this type of education could not be useful for the banks. Fraud awareness education is known to improve consumer confidence in banks, increasing their willingness to do business with them (Kim, Steinfield, & Lai, 2008). Understanding fraud protection measures in place and what to do if fraud *is* detected gives consumers more confidence in doing business. A bank that uses consumer fraud education would gain more customer trust than one that simply ignores the issue.

Increasing competition for customers also leads to increased transparency (Barth et al., 2008). This is important because, as the interviews showed, the Kenyan banking industry is very crowded and competition is very fierce, with customers having a large range of choices from small local banks to enormous multinational industrial and commercial banks. Competing for customers is therefore a distinct part of the Kenyan banking environment. Brownridge (1998(b)) argued that intensified competition in banking markets can encourage moral hazard by reducing the franchise value of the banks which represents the present value of a bank's future profits. By providing information about their fraud-fighting activities to consumers, banks can reassure their customers and increase their security, reducing churn. As observed by Bradley & Stewart (2003) banks should respond to their customer needs as customers are now of greatest importance to the banking business. Ignoring the needs and preferences of customers can be detrimental

to bank success (Agarwal et al., 2009), so if customers have a preference for increased information this should be provided.

7.3.3 External Environment Factors

The third component of the conceptual framework consisted of the external environment, which is important as it affects to what degree fraud occurs in banks. The external environment contains structural, institutional, legal, socio-economic, ethical and information technology issues.

7.3.3.1 Institutional, structural and legal issues

Legal issues included a lack of appropriate institutions and legal structures, lack of knowledge regarding fraud in the investigative and prosecution systems, and lack of appropriate laws to combat fraud. These are known issues within the literature (Aguilar, Gill & Pino, 2000; Macey & O'Hara, 2003; Wilhelm, 2004). In Kenya, the judicial and court system do not operate efficiently and there is no proper system in place for fraud case reporting in Kenya. A number of initiatives have been made to improve the judicial system through appointment of more judges, new physical facilities and amendment of relevant laws (Waweru & Kalani, 2009). However more still needs to be done to improve legislature and efficiency in the justice system, as well as reduce corruption. One of the major issues found in this study was the length of time required for prosecution, which served as a significant deterrent to its use.

7.3.3.2 Socio-economic and ethical issues

Socio-cultural issues are reflected in the acceptance of corruption as well as economic conditions that create economic stress at many levels of society (Zahra et al., 2004; Bakre, 2007). Ethical issues in banking are reflected in a sense that fraud is accepted within society, although the use of whistle-blower programs does mitigate the outcomes (Aguilar et al., 2000). This can also be mitigated by the fact that a majority of the banks maintain a written code of ethics that should be read and signed on a regular basis by the staff.

7.3.3.3 Corruption

Corruption of the police and courts was found to be another problem in this study, resulting in unfair outcomes and discouraging prosecution. This is consistent with known facts about Kenya. Transparency International's Corruption Perceptions Index, which calculates the perception of corruption within government and business environments within the country, ranks Kenya at a score of 2.2/10 (Transparency International, 2009; Transparency International, 2010). This places Kenya in the lower quartile of countries measured on the scale, indicating a very high level of corruption within business and government environments. Crucially, this implies that Kenya could have slowed economic growth. For example, research in Uganda found that bribery had a negative correlation with firm growth, with a 3% loss resulting from a 1% increase in bribery (Fisman & Svensson, 2007). This effect can be seen in banks, with banks not prosecuting those that commit fraud because of a perception that it will be futile.

The resolution for this problem is not clear. Evidence suggests that in regions with existing high corruption, an increase in penalties for cheating or bribery can actually increase bribery rather than discourage it. This is particularly difficult in cases where the inspectors and regulators themselves are vulnerable to bribes, as this will result in an even higher level of bribery (Çule & Fulton, 2009). Given these conditions, there is no clear path forward to reduction of the level of corruption that Kenyan banks must deal with in the existing system. Instead, this must be a society-wide, government-led change to reduce the overall level of corruption in society.

The Kenyan government is undertaking such a task with its Kenya Anti-Corruption Commission, which was established in 2003 to combat corruption through law enforcement, education, and development of good practices. If this Commission is successful, the Kenyan banking system should see improved conditions over time. However, the Commission is unlikely to have an immediate impact of the type that would allow banks to more effectively prosecute fraudsters in the short term. Thus, efforts through the KBA need to continue, as do internal efforts and policies. Banks should also consider that during their cost-benefit analysis, they must include effects from hiring or

transferring fraudulent employees from other banks, which could make it more cost-effective to prosecute offenders even under a corrupt system. However, this would require substantial coordination within the industry.

7.3.3.4 Ethical culture

The organisational culture within banks can either encourage ethical behaviour or create an environment where unethical behaviour thrives (Kaptein, 2008). Ethical culture was not fully explored in this study, but some dimensions of ethical culture were presented.

One issue was use of incentives to reward whistle-blowing activity. This quantitative study showed that 23% of fraud was discovered through whistleblowing or fraud hotlines, consistent with a previous study in Europe, the Middle East, and Africa, which found around 25% of frauds, were discovered this way (KPMG, 2007). This was also consistent with employee preferences for ethics hotlines rather than open door policies (Miceli et al., 2008b). However, there is some research that suggests that organisations may reject reports of wrongdoing that provide information about the organisational hierarchy, leaving employees open to isolation or other retaliation (Dworkin & Baucus, 1998). This could prevent whistle-blowing from occurring (Miceli and Near, 1985; Dozier and Miceli, 1985). Developing a culture that encourages employees and other stakeholders who identify fraudulent activities to report or take appropriate action through an ethical hotline should be a priority. Assurance needs to be given to the whistle-blower that it is good to come forward and they will be protected (Vanasco, 1998; Vinten, 1994 in Seetharaman et al., 2004).

7.3.4 Computer-Based Crimes and New Challenges

The uses and abuses of technology also stood out in the qualitative research, particularly focusing on the ways in which technology could be used for protection against fraud and the ways in which it challenged existing fraud mechanisms. There are reflections of these themes within the existing literature as well.

7.3.4.1 Technology

Information technology is reflected both in the availability of IT approaches to fraud reduction and to differentials in use and access (Fernandez & Gonzales, 2005). The relative lack of access of IT banking has reduced vulnerability on one front, although it may increase vulnerability on another. Fraud related crimes have been boosted by the introduction of the Internet and e-commerce (Seetharaman et al., 2004). Rusch (2001) also observed that there was a rapid increase in the growth of Internet fraud in e-commerce. The current research identified two issues of importance to Kenyan banks in respect to technology including the use of online banking and the problem of chip and pin cards.

7.3.4.1.1 Chip and Pin

Credit cards were the third most common fraud instrument in the quantitative study. According to press reports[3], a serious credit card fraud case occurred in Kenya involving a syndicate with fraudsters based in India, Sri Lanka and West Africa (Jayawardhana, 2009). Credit and debit card frauds originating in Europe and the Americas are beginning to be seen in Kenya. Emerging frauds are syndicate-based, and more aggressive than those in the originating country. Even CCTV or guards do not serve as deterrents. Many interviewees indicated that signature-based cards were a cause of on-going fraud, and that a lack of explicit debit and credit card fraud laws exacerbated this problem. However, most fraud in this area was related to customer card theft or fraud by customers. International credit card issuers are pushing for the use of Chip and Pin cards in Kenya as such cards are seen as a way to reduce fraud. Kenya's banking industry missed an initial target of 2006 for chip and pin implementation, retargeting implementation for 2010. This target was also missed.

Reasons for this failure are multiple. An additional cost of $8 per card would increase initial layout by the bank, which may currently outweigh the benefits (Balancing Act, 2010). Aladwani (2001) points out that inadequate resource can impede development of

[3] Daily Nation, Kenya, 25th July 2008

electronic systems. Kenyan banks could overcome the cost obstacle if they pool resources and share the cost of fraud prevention systems and technologies. However, this may not be a complete fix for the problem of card security. There is concern that chip and pin credit cards do not offer security improvements over signature cards (Finch, 2010). The introduction of these cards in the United Kingdom was at first considered to be a success, as there was a reduction in the ability to counterfeit cards or to fake authentication at the point of sale (Finch, 2010). However, fraud methods rapidly adapted (Finch, 2010). New techniques include card counterfeiting, online purchases, and stealing pins in various ways (Finch, 2010). There are also security holes that allow cards to be used without the pin, even at the point of sale (Murdoch et al., 2010). This indicates that the Kenyan banking system should not rely exclusively on chip and pin for enhanced security. Human factors training and automated fraud detection systems like Fraud Guard, currently in use in some banks, can also improve security. Other approaches include risk profile and planning, making contingency and rapid response plans, and improving training.

7.3.4.2 Online Banking

As compared to other banks in the literature review, Kenyan banks have been slow to adopt Internet banking. Gikanda and Bloor (2010) stated that Internet security is a major threat in e-banking, confirming the findings of this study. Most banks indicated that they either had not implemented Internet based banking, or that they had only implemented it in a restricted fashion, providing services for companies or elite customers. The banks felt this shielded them from much fraud, which is likely to be true given the total risk exposure of Internet banking to fraud, such as outside hackers (Lee, 2009). Automated and manual attacks often take advantages of issues like poor password choice that can be difficult to control, though this can be reduced through the use of two-factor identification (Bhargav-Spantzel et al., 2007). Internet-based fraud has already been seen in Kenya. The banking anti-fraud unit reported that in 2008, KES50 million ($641,000) intended for a firm in Dubai was diverted by hackers. In 2010, KES10 million ($128,000) was intercepted by hackers (Balancing Act, 2010).

While banks are protected from Internet attacks, they also lose competitive advantage. Bank respondents indicated they were planning to open Internet banking wider, allowing for an increased fraud exposure to more accounts. If customers view Internet accounts as vulnerable to fraud, they may not want to adopt these accounts (Lee, 2009). A recent joint survey conducted by the Kenya ICT and TNS Research International (Kenya Digital Study, 2010) revealed that 39% of respondents were interested in having access to Internet banking, but 33% considered it irrelevant. Twenty-seven per cent of respondents felt that the main barrier to Internet banking was that the service was not offered by their bank or was restricted; the same number who thought that fraud was a major barrier. This shows that banks are still limiting Internet banking, and that customers do not yet consider it essential. However, banks should begin planning for security and customer awareness to smoothly implement online banking.

7.3.5 Emerging Issues

Emerging fraud issues in the Kenyan banking industry are centred on globalization, the external environment, and cross-border fraud. This has brought about issues in international cooperation and jurisdiction. With globalization, the external environment surrounding the banking industry has grown beyond the immediate external environment. This has brought about the threat of cross-border fraud. Credit card fraud is one example of this. Respondents indicated they believed a growth in cross-border credit card fraud was likely, due to increasing exposure to international financial markets. Some banks have improved systems in anticipation, but the banking industry overall has not reacted. Efforts made by the banking industry, however, need to be supported by more robust Government legislature that can allow international fraud to be effectively tackled.

Another example is the 419 or advance fee fraud. Banks in Kenya need to be aware of this type of fraud, as it opens Kenyan banks up to international scrutiny and potential liability. Banks should consider this a major concern though monitoring it can be very difficult. Overall, evidence shows that Kenyan banks cannot only monitor domestic fraud, but must be ready to deal with international fraud.

7.4 Integration of Findings

There are strong connections between the qualitative and quantitative findings in this research. This section discusses the inconsistencies and consistencies found in this research, considering what this means for the contribution of the research.

7.4.1 Relationships between Banks and Customers

Literature suggested significant factors of competition between banks and collusion as determinants of fraud. The qualitative analysis supported these findings. The customer was the main source of fraud detection and customer-internal actor collusion was a significant source of fraud. The quantitative findings also supported these conclusions, with 70% of frauds occurring as collusion between internal and external perpetrators. The second category of perpetrators, the internal collusion, was a distant second at 13.3%. This clearly indicates that the majority of frauds are perpetrated by internal employees and customers working in unison. This would seem to conflict with findings that stated customers were the main source of fraud detection. However, this is not necessarily impossible to resolve. In particular, instances of unauthorized access to accounts, such as use of another customer's account or identity theft, ranked high in the ways in which fraud was perpetrated. Simply, this suggests that the customers identifying the frauds as victims are not the same customers or other external factors that are serving as perpetrators.

A second significant relationship is between banks themselves. One issue in fraud is competition between banks for customers and employees, which often results in the banks accepting unknown or unacceptable risk. However, the banks also cooperate through the KBA. There are no quantitative figures on how many banks participate, though the qualitative findings indicate that there is widespread involvement. However, information and participation is uncertain and banks do not have a consistent view of the purpose of this involvement, making it less effective overall than it could be.

7.4.2 Prevention and Detecting Fraud

The issue of preventing and detecting fraud was significant in both the qualitative and quantitative findings. The quantitative findings showed relatively high levels of use of industry-standard fraud detection mechanisms, including audit committees, ethics policies, and advanced technologies like data mining. However, the qualitative findings indicated that these methods were not necessarily effective. In particular, respondents mainly used job rotation and the segregation of duties as the main methods of fraud prevention, detection and control. The absence of fraud budgets or the inconsistent funding due to inability to predict fraud reflect that more needs to be done by banks to streamline planning and resources required to counter fraud.

7.4.3 Structural and Institutional Issues

The rates of criminal prosecution for fraud are low with just 30.9% of primary internal colluders being referred for criminal prosecution. Qualitative findings revealed that Kenyan law enforcement and legal structure and institutions are insufficient to the task of fraud prosecution. Issues like out-dated or missing laws, lack of knowledge and training, court inefficiency, and corruption make many banks avoid prosecution. This indicates a significant problem that cannot be resolved within a bank or even within the industry, but that needs to be assessed at an institutional and society-wide level.

7.4.4 Computer-Based Crimes and New Challenges

The quantitative findings suggested that banks were using computer-based technologies like antivirus and passwords commonly, though other approaches such as data mining and digital analysis were far less common. The qualitative findings indicated that banks did not currently face much in the way of online threats, although these were growing, because of limited use of online banking technologies. However, these are only likely to grow over time and the development of approaches to combat them is not currently on the horizon, from the qualitative findings regarding the matter. This could pose a significant threat in future.

7.4.5 General Integration of Findings

Integration of qualitative and quantitative findings can lead to several conclusions. First, relationships are key to understanding the problem of fraud and fraud detection in the banking industry. Issues like collusion influence how fraud can be detected, while industry strength and involvement influences the ways in which fraud can be prevented on a larger scale. However, industry involvement, such as KBA participation, is uncertain at best and suffers from a number of flaws such as inconsistent information. Second, the fraud detection structures put into place in the banking industry may seem to be consistent with the current best practices, but in practice they can be shown to be underfunded and inadequate. Third, institutional and legal insufficiency does not allow for effective fraud prevention, limiting the recourse banks have to legal avenues. Finally, new technologies can both help prevent fraud and exacerbate it, offering new challenges. At the current time, Kenyan banks are not fully prepared to face these new challenges, although banking managers are aware of the gap between challenge and involvement.

7.5 Differences between International and Other Banks

Findings in Chapter 6 indicate a number of differences regarding treatment and perceptions of fraud between international banks and banks with a smaller scope (though these differences did not emerge in the quantitative findings). Closer involvement in the KBA and greater use of technology for fraud detection are notable. These differences are reflective of key issues in African business and its integration with Western firms, particularly differences in human resources and capital. The Kenyan banking industry is not idiosyncratic, but is instead influenced by the external environment of African and global business. These differences can be examined within the current literature in order to understand how the Kenyan banking industry is not an idiosyncratic environment, but is in some senses a microcosm of the wider African business world. This section focuses on these differences.

7.5.1 Industry Involvement

One qualitative observation was that international banks are far more involved with the KBA, taking active roles on the Securities and Fraud Committee. This contrasts with

domestic banks, which mainly play a more passive or support role. The KBA acts, among other roles as an information sharing body. International bankers generally showed a stronger understanding of the purpose of the KBA and involvement in its activities, as well as knowledge about its meetings. However, other banks did not show this level of knowledge. For example, one senior auditor at a regional bank expressed only a vague awareness of the meetings that took place, in contrast to expectations that she would know about the Securities and Fraud Committee even if she were not personally involved. It is possible that this could be due to size and availability of resources for fraud detection, or that this could be someone else's duty. Regardless, these findings indicated that the overall level of involvement in the KBA was substantially different between international and domestic banks.

Observed differences could be explained by size. Research into structural differences between large and small banks indicates that large banks tend toward a more rigid institutional structure and less informal information sharing and development (Berger et al, 2005), which could influence their choice of formal or informal networking, while smaller banks chose to use informal and soft information channels. However, smaller banks are highly vulnerable to failure from fraud compared to larger banks (Mishkin, 1999), which could negatively affect the position of small banks.

There is also likely to be a geopolitical issue involved. Historically, banking institutions in Africa have been relatively weak compared to the international market (Stein, 1994). This institutional weakness dates to the colonial period and the foundation and domination of banking systems by international banks (Stein, 1994). Historically, no such institutional boards existed prior to the structural adjustment and market liberalization programs of the 1980s (Neu et al, 2010). Thus, structures like the KBA are relatively new. The African banking system was also unstable much of the time from 1980 to 2000 due to fraud and government corruption (Kane & Rice, 2001). Conditions of historical weakness and vulnerability to fraud, along with environmental conditions that could promote fraud, indicate that local and smaller banks could benefit from KBA

involvement. The KBA should also be proactive in developing ties to the domestic banking market and establishing legitimacy.

7.5.2 Knowledge and Human Capital

International banks generally showed a generally higher level of knowledge and ability to manage fraud than do domestic banks, including full-time fraud detection personnel. International banks are also more conversant with institutional reform issues. For example, international banks were more likely to identify unskilled prosecutors, rather than the more visible police or general courts, for failures in prosecution. International banks also have an objectively higher standard of human capital. For example, they hire members of the Association of Certified Fraud Examiners (ACFE), who have higher and more up-to-date skills. However, this has not prevented all fraud in international banks. There is the possibility that greater cooperation would bring about sharing training and expertise through the industry.

These issues point to the problem of human capital development (HCD), or development of skills and resources required for economic growth, which is a structural problem that is endemic to many African economies including Kenya (Patterson, 2007). In fact, differences in the efficiency of manufacturing and production in sub-Saharan countries have been largely shown to be attributable to different levels of human capital development (Bigsten, et al., 2000). HCD is required to trigger demographic transition (marked by lower mortality rates, longer lifespan, and lower birth rates) and industrialization (Tamura, 2006). The lack of HCD affects economic growth in Kenya generally, not just the banking industry. The lack of HCD is apparent in the failure of awareness of Basel II in banking institutions (Bank Supervision Annual Report, 2008).

There are a variety of approaches the banks could take, although the problem of HCD is outside their direct control. One approach is seeking technical assistance and/or hiring Western fraud investigators to improve fraud response. The use of technical assistance is routinely used in African banking systems, before and after structural adjustment (Oshikoya, 2010). This would improve internal human resources. Hiring Western fraud

investigators would be relatively expensive given wage differentials and would not provide sustainability, making it a short-term solution. Banks could also invest in human resources training themselves, an approach frequently taken by African companies (Kamoche, 2011). The on-going and sustainable development of required human resources is a broader societal issue that must be addressed at the state level to provide banks with access to suitable HCD.

7.5.3 Capital and Technology Resources

There are marked differences that can be observed in terms of resources. International banks are far more likely to have a fraud budget. Domestic and regional banks do not tend to have a specific fraud budget, and instead treat fraud as an on-going operating expense or ignore it completely. The CBK indicates that 60% of banks have set specific risk management budgets, up from 17% in 2004. Around 50% are setting aside amounts of up to 10% of their annual turnover for risk management This shows that most banks are beginning to assign more importance to risk management functions. However, 40% of banks do not yet have specific risk management budgets (Risk Management Survey, 2010).

International banks are more likely to use technology, such as automated fraud detection and prevention systems. They more commonly offer online banking and telephone banking. These differences point to a significant difference in the two levels of banks in their available capital and technology resources in order to implement fraud detection.

One of the major problems in this case is lack of capital for development of effective fraud programs. It should be recalled that Kenya is not devoid of resources with which to generate capital for business investment. Some countries like Angola have high revenue levels generated by natural resources. However, problems of capital flight and expatriation of funds from these resources mean that redistribution of capital is insufficient for growth (Frynas & Paulo, 2006). Kenya's main resources come from tourism, export of tea, coffee, horticultural crops and industrial exports of refined petroleum. If re-distributed strategically these resources can provide capital resources for

technological development. However, this is not the only problem that African businesses in general, including the banks in this study, face when considering access to capital.

Corruption is a serious problem, which limits Western investment and business involvement (De Maria, 2009). Corruption is also connected to technology. Foreign direct investment (FDI) and joint venture partnerships are major vehicles in technology transfer, or the transfer of specific knowledge sets and technology uses from firms in developed countries to those in developing countries through licensing, patents, and development of business processes (OECD, 2002). However, political instability including corruption is likely to inhibit FDI and reduce technology transfer (Asiedu, 2006). Limitation of technology transfer from perceptions of corruption could reduce banks' ability to access and use technology, resulting in overall lower technology use. However, banks also have other restrictions. For example, data privacy laws and other restrictions on interaction between banks could limit the degree to which a bank could engage in a meaningful joint venture partnership or FDI relationship with an international firm. However, it should be considered that overall lower levels of access to human capital, financial capital, and technology, rather than simple ignorance of or rejection of the importance of fraud detection within the bank, is far more likely to lie at the heart of this problem.

7.5.4 Implications of Differences for the African Banking Industry

Differences between domestic and international banks include identified structural problems with human capital development, financial capital availability, and technology availability that led to conditions under which the African banks in this study did not have as high a level of involvement or integration of technology as their international counterparts. These differences are connected to international economic conditions, including resources and business models. However, there are also historical and structural implications of these differences.

These differences can be traced to structural adjustment programs and market liberalization. Structural adjustment was implemented in Kenya in the early 1980s,

liberalizing markets and lowering trade barriers. This was intended to increase the competitiveness of Kenyan companies and institutions through exposure to the outside world, and to move the economy from a dependent economy to one that was fully integrated into import and export structures (Mohan et al., 2000). However, this was not the result. Kenyan banks are disadvantaged in terms of size, resources, and technology compared to international banks. Insufficient HCD means that fraud detection cannot be sustainably implemented. With these challenges, banks have limited options for improving their performance. Approaches like technical assistance, hiring international specialists, or setting up a training program cannot be implemented without access to appropriate capital, which is not available from partners due to perceptions of corruption overall. This is not a problem that can be solved by the bank, but must be addressed by Kenyan society as a whole.

7.6 Qualitative and Quantitative Findings in Relation to Theories of Fraud

The economic and general theories of fraud can be used to consider the findings of this study, to determine how these findings relate to the existing theoretical frameworks. The intention is also to determine how the research could be used to expand the existing theoretical base in order to account for the findings identified. The qualitative and quantitative findings both have some implications for the theories of fraud that have been identified.

7.6.1 Theories of Fraud

Criminological, economic, and accounting theories of fraud have all been previously discussed, and each can be applied in this case.

The basic theory of fraud is the theory of differential association (Sutherland, 1949). However, the main model applied in this research is the fraud triangle theory (Cressey, 1973), which has been discussed extensively in this research. A refinement on the fraud triangle theory is the fraud scale (Albrecht et al., 1984; Albrecht, 2004), which substitutes integrity for rationalization. An extension of the fraud triangle, the fraud diamond, adds ability of the offender to commit the fraud (Wolfe & Hermanson, 2004). In addition to

the basic four factors of pressure, opportunity, motivation, and ability, this study has identified a fifth factor, collusion, which relates to almost 90% of frauds in the Kenyan banks.

Main economic theories of fraud include agency theory and control fraud theory. Agency Theory holds that there is a fundamental problem with situations in which there is a principal-agent relationship (Stremitzer, 2005). Control fraud theory holds that in some cases, the entire structure of the organisation may be designed so as to facilitate fraud by specific agents within the firm, such as top managers (Davia et al., 2000). Agency theory may have some application, but there was no indication of control fraud evident in cases studied.

Eclectic theories integrate a number of disciplines Riahi-Belkaoui and Picur (2000) identify a framework that integrates ecological theory, transmission theory, and anomie theory in order to identify situations where fraud is most likely to occur. However, the utility of these theories in this case is somewhat limited, with considerable disagreement regarding the application and characteristics of fraud profiling or simply echoing the fraud profile (Hollinger & Clarke, 1983; Steane & Cockerell, 2005; Weisburd et al.., 2001). Thus, these studies are not discussed in detail.

7.6.2 Criminological and Sociological Theories

A basic application of the theory of association can be seen in collusion. Collusion between employees was the second most common situation in which fraud occurred, which is consistent with the theory of differential association, as were cases where associates, ex-co-workers, and others were co-conspirators. Although communication between participants clearly occurred, the study did not address the process of collusion. Thus, more comprehensive statement regarding the differential association theory cannot be made. Given that the theory of differential association is one of the most broadly accepted and applicable theories (Wells, 2005), the application to the research environment is justified. However, this theory cannot explain why fraud has occurred.

The fraud triangle theory and its extension, the fraud diamond theory, are less limited. These theories posit that the commission of fraud is due to factors including opportunity, motivation or pressure, and rationalization, or in the case of the fraud diamond ability to commit the crime (Cressey, 1973; Wells, 2004; Wolfe and Hermanson, 2004). This theory can be seen to be extremely relevant to the current situation, given the motivations identified by those that have committed frauds as well as the rationalizations that were determined.

The necessary prerequisite of financial fraud is that the individual must have the opportunity to commit the fraud; that is, they must be in a position of financial trust in order to commit the crime (Cressey, 1973). Of the three aspects of the fraud triangle, opportunity is the most observable or measurable element. In the past opportunity has mainly been investigated in the light of weak internal controls and segregation of duties (Dorminey et al., 2010). In this study, this could be applied to the bank customer(s), because the customer is in a position of limited financial trust due to the acceptance of their business by the bank. Customer frauds involved false identity documents and counterfeit or fake cheques, promoting trust. In a bank environment, there is some degree of trust associated with almost every position. Thus, the vast majority of the fraud perpetrators within the study do fall within the purview of this theory in terms of the opportunity to commit fraud. Factors that contributed to creating opportunity included weak internal controls, overriding of internal controls, poor or lax supervision, failure to segregate duties, failure to know the customers (KYC), easy access to customer accounts and taking employees taking advantage of trust vested in them as workers. However, this research revealed that opportunities such as lack of prosecution, the absence of effective anti-fraud programs and the ability of fraudsters to get re-employed were important considerations as well.

The second leg of the fraud triangle is that of motivation, or the reason why the crime was committed. The main motivation identified by Cressey (1973) was a non-shareable financial strain, such as that attributable to financial isolation, poor investments, excessive spending, or problems such as drug abuse or gambling. A second motivation is

organisational dissatisfaction (Hollinger and Clarke, 1983). This motivation can be seen as a type of extension of anomie theory, in which the fraud perpetrator engages in fraud due to a lack of connection to the organisation specifically and the idea that they are not getting their fair share of the organisation's resources (Wells, 2005).

In fact, all of these motivations can be seen to be present in the fraud motivations that were identified in the quantitative study. There were two particular findings regarding "pressure" as a part of the fraud triangle. First, based on the respondent's views, pressures like lifestyle habits, financial pressure and greed scored highly among the fraudsters as triggers for fraud commission, validating the fraud triangle. The absence of substance abuse and failing sets the findings apart from the literature (primarily based on Europe, America, and Australia). This could be attributed to differences in society and lifestyle, in particular differences in collectivism, socioeconomic status and the importance of family. In Kenya, the extended family is more important than the Western nuclear family or individual. Many of the motivations, such as increasing school fee pressure, were family-related. It can be argued that pressures such as substance abuse and gambling are predominantly individual, though they can be related to peer pressure. Additionally, habits like drugs and gambling are expensive. With over 50% of its population living below the poverty line, these would be very expensive habits and not within reach. This could explain why gambling and substance abuse score low as pressure points for committing fraud in Kenya. However, it could also be that perpetrators did not disclose these activities to fraud investigators.

Secondly, this study exposed an unclear line between opportunity and pressure. In the questionnaire, among the choices given for motivators of fraud, "opportunity" was inbuilt as a distracter. "Opportunity" was mentioned by most participants making it the number one pressure, higher than financial pressure and lifestyle habits. This could imply that the three legs of the fraud triangle are not perceived as being distinct and therefore it follows that given sufficient opportunity, fraud did not require uniquely identifiable social, financial or organizational pressure for its occurrence. It also provides support for the theory of the accidental fraudster versus the predator (Kranacher et al, 2011), in which

there is a difference between generally good people pushed to commit fraud and those that seek out opportunities for fraud. The phenomenon of the serious fraudster seen in this research also reflects this theory. However, there was little support for organisational dissatisfaction theory, such as being underpaid of revenge (Hollinger & Clarke, 1983).

The final leg of the fraud triangle theory is that of rationalization (Cressey, 1973). Some rationalizations include excessive need, identification of the fraud as good for the company, and a feeling of unfair treatment. These responses were considerably more mixed in this study. The most common rationalizations included a desire to get rich, family pressures, and an environment in which everyone else was engaging in fraud. The desire to get rich is consistent with an entitlement rationalization, in which the participants feel that they are entitled to a better lifestyle or more of the bank's resources than they are currently being paid. This rationalization is not explicitly identified within Cressey (1973); however, it has emerged in later empirical studies on the problem of fraud, that this rationalization is common (Wells, 2005). Of course, the claims of family problems are also consistent with the rationalization process, as participants will come to believe that they do not have an alternative to maintain their family's position.

Capability, added by the fraud diamond model (Wolfe & Hermandson, 2004), speaks to the individual abilities and personal characteristics of the perpetrator, including the ability to perpetrate and cover up the fraud. All internal perpetrators in this research were employees who had access to cash paid in, applications for loans or had privileged access to customer account information; for example cashiers or tellers, verifiers, computer operators, receptionists, front office and back office accounting clerks, supervisors and staff is some junior and senior management positions. Some were also familiar with internal controls or trusted with ability to override them. External perpetrators commonly had access to inside knowledge through collusion, or in one case as an ex-employee. These findings offer support for the addition of ability to the model.

One problem with this research is the use of second-hand reports to provide evidence for pressure, opportunity, and rationalization. (It is presumed that capability can be

adequately reported by banks aware of access and skills.) This is obviously problematic since what was reported to the banks may not actually be reality. However, the fact that pressures were not known does indicate that better knowledge of employees is called for. (Of course, it is also possible that there were no explicit pressures, as noted above.) This requires stronger HRM practices by banks.

7.6.3 Economic Theories

The agency theory can be seen to be highly applicable within this research area. The general findings indicated that the most common fraud was that conducted by insiders within the firm, or by collaboration between external and internal parties. The respondents did not generally indicate whether these were individuals in positions of authority, but to a certain extent this is irrelevant; for example, a bank teller that has power to control cash intake within a bank acts as an agent for the bank, and thus there is still a principal-agent problem. Lending malfeasance (Barth et al, 2009), where the lending officer is authorized to act as agent for the bank, is a common area of agency theory application, though this was not identified in this research (though it likely has occurred). However, this does not provide personal motivations for fraud, as do criminological theories like the fraud triangle/diamond, making it less satisfactory.

7.6.4 Eclectic Theories

The theory proposed by Riahi-Belkaoui and Picur (2000) indicated that fraud arose from internal and external conditions and one condition is that the bank may present an external face of being competent dealing with fraud that does not reflect the internal reality. This can clearly be seen to be the case within the banking industry as a whole as indicated by the interview material. For example, while the KBA was presented as a major self-regulatory effort, some respondents from smaller banks were only marginally participatory or aware. The participants indicated that there was ambivalence regarding public disclosure and information sharing, indicating concerns regarding the problem of scaring the public or seeming to be weak in their treatment of fraud. These responses clearly indicate that the banks in the study are generally not actually in control of their fraud situation, but instead are using the promotion of activities like the KBA's Securities

and Fraud Committee action in order to disguise ineffective management of fraud in the internal organisation. This is the necessary precondition, according to this theory, and thus is highly important in introducing institutional conditions in which fraud could occur.

Another condition required is an environment in which institutions have unequally distributed power, leading those that are not members of these institutions to ignore the problems that emerge within the organisation due to the perception of increased power (Riahi-Belkaoui and Picur, 2000). This is the case in Kenya, where a high rate of poverty associates the banking industry with power and wealth, isolating it from requirement for an effective regulatory and institutional environment. This is exacerbated by Kenya's structural adjustment program, in which the regulation of the financial services industry was seen as a detrimental factor in the country's growth and so much strict regulation and oversight by the government was removed (Mohan et al., 2000). Thus, in the case of the Kenyan banking industry is insufficient oversight and transparency driven by competitive concerns, creating conditions for secrecy regarding fraud.

A third condition is an internal lack of social organisation (Riahi-Belkaoui and Picur, 2000). This is absolutely a condition in the study. Interviews indicated that there was no independent way to clearly identify someone that had been previously convicted of fraud or sacked due to fraud; although the KBA was said to be working on a database that would allow for tracking this, it had not yet been prepared and did not have a clear delivery date. While banks relied on personal recommendations, a culture of secrecy and failure to provide these recommendations made these unreliable. Criminals could be attracted to the banks knowing they would not be immediately detected (tying in with the predatory theory discussion in section 7.6.2).

Under the above three conditions, the organisation develops a culture in which fraud is endemic – that is, everyone is seen to be corrupt (Riahi-Belkaoui and Picur, 2000). This eases rationalization, as fraud is seen to be tolerated. Lack of effective regulation as shown in this study, must increase this perception as well, since there is no way to

determine whether one's co-workers are engaged in fraud (except for collusion). This organisational climate is reflected in many of the justifications for the fraudulent activity that were disclosed. It also reflects on the high rate of collusion between co-workers, which also reflects on differential association theory as discussed above. However, this is not just a bank culture problem, but a society-wide problem, that must be addressed at a higher level.

7.7 Socio-cultural, Legal and Economic Issues

The findings touched on a number of socio-cultural, legal and economic issues that affected the practice of fraud in the Kenyan banking industry. Some specific issues that have been identified include lack of institutional capacity to allow for successful prosecution, ethical issues, and economic issues that may come into play in the outcomes of the fraud investigation.

7.7.1 Institutional Capacity and Legal Structure

One of the major issues identified by participants is a lack of institutional capacity on the part of the Kenyan government to deal with the problem of fraud. Some of the problems identified included lack of interest, capacity and skills on the part of police and prosecutors, an inefficient and ineffective court system, and lack of sufficient laws to address problems like credit card fraud. This inadequacy in the Kenyan laws revealed through this study supports research on e-banking done by Gikanda and Bloor (2010) who found that the absence of clear legal regulations in Kenya poses a challenge of significant importance in the banking industry. Problems including lengthy and expensive proceedings, long recesses, and long periods between fraud identification and prosecution led to reduction of willingness to prosecute on the part of banks, which often used civil settlements or dismissal instead. However, many of the participants expressed frustration with this, and indicated that they would prefer that there was a consistent legal approach in place that they could use.

The legal external environment, including laws, regulations, and institutions (Aguilar et al., 2000) is obviously going to be one of the major factors in how well banks can fight

fraud using a legal enforcement approach. Legal enforcement can occur at the local, national, or international level (Macey & O'Hara, 2003). The majority of issues in this case were national, with low international involvement. Issues such as corporate governance (Licht et al., 2005) and development law (Doidge et al., 2007) did not emerge explicitly during this review. However, two areas that did emerge were the legal environment for lending (Barth et al., 2008) and the availability, commonality, and competence of police investigation and criminal prosecution (Wilhelm, 2004) most especially. Thus, these findings were consistent with the expected outcomes in terms of the sources of fraud and their determinants.

The weakness of laws related to banking fraud in Kenya is not unique. In fact, the conflict and consensus approach to fraud identifies weak structural regulation of white-collar crime such as fraud as the outcome of institutions wanting to appear to be in control when in fact they are not (Carey, 1978 as cited by Riahi-Belkaoui and Picur, 2000). Under this model, the social inequalities that cause conflict are also responsible for lack of effective legislation in order to prevent the crime from occurring. Under the ecological model of fraud, fraud actually occurs in the banking industry because the industry is the site of social disorganisation (Riahi-Belkaoui and Picur, 2000). Kenya may be particularly prone to social disorganisation due to general weakness and disorganisation of special interest groups, including accounting associations and the KBA, which could otherwise promote the banking industry's interest in making laws. While larger international banks reported both KBA involvement and willingness to prosecute (likely due to greater resources), the KBA itself is not taking any definite measurable steps in improving legal institutions or provide training for prosecutors or policy. They have taken small steps, like advocating for Credit Reference Bureaus. However, there is significant room for improvement. This general weakness is consistent with the ecological theory of fraud.

7.7.2 Sociocultural Issues

A second area of concern that was seen in the qualitative and quantitative findings is the reflection of sociocultural issues, such as ethics and the general acceptability of

corruption and fraud, within the banking industry and society as a whole. Main sociocultural issues seen include the business environment and its conflict with cultural norms, the use of collusion and the social position of fraud as something that need not be hidden, and the overall prevalence of corruption. The bank's use of ethical training is likely to be insufficient to overcome these problems.

Ethical factors are social norms and values internalized by the individual that allow for acceptance of fraud by that individual (Aguilar et al., 2000). Ethical practice is a cultural issue, not only an organisational value. While it seems that ethical values should provide guidance against fraud, in fact ethical values can at times become twisted in order to allow for rationalization of fraud under the fraud triangle theory (Cressey, 1973; Wells, 2005). For example, a worker that is underpaid may rationalize that he or she is not getting paid what he or she is worth, and that is unfair; in this case, fraud serves as a means of rectifying the disparity between the worker's pay and their perceived self-worth (Wells, 2005). However, broader sociocultural norms can also play into the use of fraud in the industry; for example, if fraud is considered to be acceptable business practice, or is overlooked or ignored by employers or faces a relatively light treatment when discovered, it may well become endemic due to its general acceptance (Zahra et al., 2007). The acceptance of corruption within a given society is of particular concern, since this is likely to allow for justification on a wider scale by the individual engaged in fraud (Bakre, 2007).

This is particularly likely to be a problem where there is an existing environment of corruption and fraud. This was found to be the case in both the qualitative and quantitative findings. The persistence of collusion between co-workers also indicates that there was an environment in which there was a general acceptance of fraud. Finally, respondents indicated that corruption and bribery in the legal system itself were frequent causes for concern and were a major reason why the banks might avoid prosecution. This all indicates that there is a breakdown of ethics within the banking industry, as well as possibly within Kenyan society in general, that allows for fraud to take place. Thus,

fighting fraud within the Kenyan banking industry is not only an issue of changing corporate culture, but of changing the broader sociocultural norms.

There were also economic issues involved in frauds reported, such as economic strain. This type of economic strain is consistent with the first leg of the fraud triangle, the non-shareable financial problem (Cressey, 1973; Wells, 2005). While there were a number of other factors cited, including overconsumption and greed, the problems of high unemployment and low wages must be taken into account as potentially major sociocultural issues in the overall prevalence of fraud, since they will deliberately reflect on the use of fraud in the banking environment. This is particularly true for external perpetrators (as internal perpetrators have gainful employment).

7.7.3 Industry Issues

The banking industry itself must be taken to task for its own practices, many of which promote fraud. In particular, circumvention of Know Your Customer rules, lack of industry involvement in the KBA and lack of information regarding KBA activities, and failure to check references for new employees are all significant elements in the exposure of the Kenyan bank to fraud. The use of slipshod employment and customer verification practices by some of the Kenyan banks offers the opportunity that individuals need to commit fraud (Cressey, 1973; Wells, 2005). Banks need to take responsibility for their own hiring and customer recruitment practices in order to eliminate this opportunity. Although some banks have undertaken steps such as establishing whistle-blower hotlines (Black, 2005b; Schmidt, 2005) or ethical training programs (Aguilar et al., 2000), these programs are not sufficient.

In essence, the current treatment of fraud by the banking industry in Kenya is consistent with the eclectic theory of fraud, in which the industry indicates they are taking private action to prevent fraud, while continuing to contribute to conditions of extreme social inequality; failure to apply pressure in order to create conditions for social control in the broader society; allowing conditions to continue to exist where fraud and white-collar crime are considered to be acceptable; and failing to report or prevent fraud from

occurring (Riahi-Belkaoui & Picur, 2000). Given this failure, banks must be held accountable for the environment that they have partially created and have failed to change substantially in order to prevent fraud.

7.8 Broad Implications of Findings

The findings demonstrate that, above all, the problem of insider fraud in the Kenyan banking industry is not simply a failure of the individuals, the banks involved, or indeed the banking industry. Instead, it is a broader social problem that is related to government policy and institutions as well as the general development of the Kenyan banking institution. The development of the banking structure and system means that the banking institution, perceived as being one of the elite institutions, is isolated and does not have access to outside resources to control fraud or pressure toward transparency. However, this is not only a matter of elitism, but of structural adjustment and resulting deregulation. Given this, the Western bias of the eclectic model discussed is exposed – it takes into account conditions under which deregulation has taken place, but does not address the legitimate role of regulation in fraud prevention.

In general, the findings were largely consistent with the requirements of the Fraud Triangle and Fraud Diamond Theories and to a lesser extent the agency theory, differential association, and the eclectic theories discussed in the literature review. One significant factor that stood out and emerged from the research is the extent of insider fraud and collusion. From this study the presence of collusion, in essence, adds an extra dimension to the fraud elements identified in other studies. These findings also pointed to a connection between the internal organisational culture and the external environment, demonstrating that even though the findings point to conditions within the bank, they also reflect issues that are seen in wider society and that need to be addressed there. Of particular importance are the KBA and its fraud-related actions. It can be seen that, rather than taking the leading role expected, the KBA serves to present a veneer of treatment of issues on security over a general lack of involvement and knowledge. The KBA should take the lead in development of robust fraud prevention measures in the banking industry which will go a long way in tackling the fraud threat. One overarching point is that fraud

cannot be viewed solely from the perspective of the individual. The organisation and the wider environment play a role in creating conditions for fraud to occur. Thus, the individual perspective is insufficient to explain the occurrence of fraud.

7.9 Managerial Implications of Findings

There are a number of issues relating to best practices in the banking industry. While internal fraud is clearly a concern, many banks do not take appropriate steps to prevent internal fraud from occurring, consistent with previous research (Brancik, 2007). For example, password security is used in most cases despite its known security weaknesses (Payne & Richards, 2008), leaving banks believing they have a higher level of security than they do. A more robust approach is two-factor identification, which uses something that a user has (like a number generation token or smart card) and something that the user is (like a pass-code, image recognition, PIN, or biometric identifier) to authenticate (Bhargav-Spantzel et al., 2007). This type of security is substantially more secure and less prone to failure than some single complex password identification. This is slightly more costly, and so has been avoided by incomplete cost-benefit calculations. However, banks should revise this stance in light of current conditions.

Secondly, strategic frameworks can be used within the banks to boost the development of an effective approach to fraud management. Adams (2010) suggests the Prevent, Protect, Pursue framework:

Prevent: Take measures to prevent fraud and detect areas of vulnerability before attacks happen. Implement correct procedures and ensure they are followed, train staff, and adhere to industry initiatives.

Protect: Protect infrastructure against security breaches and implement warning systems to warn against them.

Pursue: Follow best-practices guidelines and set standards for dealing with offenses.

These practices allow banks to prevent further breaches (Adams, 2010).

This basic framework provides a robust guidance for banking implementation of best practices and ensuring that the appropriate technical procedures are in place in order to

allow for the appropriate structure of banking standards and protective practices. Thus, the identification and correct implementation of strategic practice should be a key determinant in how banks prevent fraud.

Thirdly, organisational culture has been found to be a determinant in a large number of cases of widespread internal fraud or malfeasance. Sometimes, organisational culture is such that participants believe the organisation to be effectively combating fraud, while at the same time fraud is allowed by policy variance (Smith & Drudy, 2008). A remedy for this is retraining managers to promote and enforce the policies that are in place, thus changing the corporate culture to ensure that it is more in line with the actual demands of the organisation (Small, 2006). Thus, banks that demonstrate this problem of lack of alignment between standards and practices should focus on improving this alignment in order to be better able to combat fraud.

Fourthly, the KBA is representative of a self-regulatory organisation (SRO), which are held up as major mechanisms for the reduction of fraud and corruption within an industry (Nunez, 2007). SROs operate on the principle that industry regulation by the members of the industry itself is a far more important mechanism than government regulation, that it is less expensive, and that it is more effective than government regulation. This has been shown to be the case, with even corrupt SROs, which are vulnerable to bribery, having a higher level of self-regulation than industries that do not have this type of organisation (Nunez, 2007). Kenyan banks have an opportunity through the KBA to do more in sharing information, such as the credit information sharing initiative, such as that available in other regions. At least 14 countries in Europe have public credit registers while all member countries have private credit bureaus (Giannetti et al., 2010). So far Kenya has only launched one credit bureau, which will reduce information asymmetries regarding customers. This success can be expanded. By working together and sharing fraud information the banks can enjoy a degree of transparency, enhanced stability, healthy competition and lower shared costs for screening and monitoring fraud (Giannetti et al., 2010; Mwanza, 2010). Not only should Kenyan banks endeavour to create adequate information sharing on fraud within the Kenyan banking industry, but should also

consider regional and international information sharing. This will assist in facilitating cross-border expansion as foreign banks can readily access data and information on the same footing with the local banks, as well as reducing cross-border fraud.

7.10 Reflecting on the research questions and conceptual framework

The qualitative study brought out a few characteristics of fraud in part answering Research Question 1. This captured the main types of fraud, the amount of fraud loss, reporting and recovery of fraud. These aspects were discussed in Chapter 5 and were therefore not pursued again for discussion here.

This chapter has also followed up discussion based on Research Question 2 about characteristics of those who perpetrate fraud. From the onset in this chapter, research question 2 has been discussed highlighting the individual perpetrator as well as giving consideration to collusion and the concerns about internal controls. The characteristics of fraud perpetrators are discussed further revealing the centrality of the fraud triangle in individuals who commit fraud – pressure, opportunity and rationalization. To these characteristics the discussion incorporates two other characteristics, capability and collusion ending with a discussion on what can be done internally to minimize fraud and fight collusion making way for a discussion on the importance of internal controls. In answer to this research question the findings and subsequent discussion in this chapter indicates that other than the elements of the fraud triangle, capability and collusion are additional elements that should be considered in understanding fraud in the banking industry in Kenya. Also the nature of the perpetrator does not always fit the fraud triangle as results show that some perpetrators have a predatory nature and therefore do not fit the 'accidental fraudster' that the fraud triangle was created to suit.

Drawing in the discussion on internal controls leads us into Research Question 3 on how banks approach fraud management. The discussion highlights the significance of internal control systems in fraud management – job rotations, separation of duties and responsibilities, internal audit, screening and recruitment procedures and systems controls. The discussion later extends to fraud prevention and detection.

Research question 3 is also answered in the discussion on the difficult balance between industry co-operation and competition for customers. Customer education is also addressed as an aspect of customer fraud awareness. These all have implications on fraud management as do external factors such as technological, socio-economic, ethical, institutional, structural and legal issues discussed.

Research Question 4 is addressed for the first time in this chapter. Section 7.5 attempts to give an answer to the question "Are there differences between the approaches to fraud management adopted by Kenyan and international banks?" The discussion is built on findings of this research that point to differences in the way banks respond to industry involvement, access to knowledge and human capital, access to capital and technology resources and the broader implications of these differences for the African banking industry.

Sections 7.4, 7.6 and 7.7 cut across Research Questions 2 and 3 discussing further issues earlier raised, integrating the findings and linking the same to theories and literature in fraud.

The conceptual framework can be traced through Section 7.3. Section 7.3.1 reflects on the individual and the fraud triangle which is the central aspect of the conceptual framework. The internal factors representing the bank and the industry in the conceptual framework are discussed in Section 7.3.2 while the external environment factors of the conceptual framework researchable through this study are discussed in Section 7.3.3. Section 7.3.4 captures the information technology factor which is part of both the internal and external factors. As with the research questions, Sections 7.4 to Section 7.7 addresses a range of factors from the three aspects of the conceptual framework.

7.11 Summary

The findings of the qualitative and quantitative research had some important implications in terms of their connection to the literature. The findings were consistent with the

conceptual framework, although there were several emergent themes not included in the model.

The structural and interpersonal relationships within the banking industry play a clear role in determining both the occurrence of fraud and its prevention. However, these relationships, particularly intra-industry relationships such as references and the KBA are not being used effectively to prevent fraud. Fraud detection also suffers from issues such as lack of dedicated resources and unavailability of predictive mechanisms. Although the interviewed fraud managers show a strong awareness of what they should be doing, they do not have the available resources to do so. A third issue and perhaps one of the most significant issues because it cannot be rectified through bank or industry level changes, is the failure of legal institutions, which make it extremely difficult to prosecute fraud in a timely or cost-effective fashion. Finally, there are a growing number of technology changes that could both encourage and prevent fraud. Banks need to focus more on preventative technologies in order to prepare for the development of incoming threats, which are already beginning to be seen within the industry.

Chapter 8

Conclusions and Recommendations

8.1 Introduction

The aim of this study was to make a contribution to the understanding and knowledge of fraud in Kenya. The research that has been discussed within this study was broad-ranging and detailed, and addressed a wide range of fraud-related issues in the Kenyan banking system. However, this only reflects a partial view of fraud in the Kenyan banking system, with only minimal discussion of the historical and colonial nature of the banking system addressed. There is a deep substratum of political, social, and historical issues that fell outside the scope of this discussion, which has focused only on the banking practice aspects of the problem. Even considering this, the information produced within this review offers a significant basis for comparison of the Kenyan banking system with the banking systems of other countries, as well as exploring many of the issues that are found within this system. This chapter discusses the theoretical and practical contributions made in this research, summarizing the main findings in regard to the research questions (Section 8.2), discussing contributions to knowledge, theory, and literature (Section 8.3), discussing policy implications and recommendations (Section 8.4), and discussing limitations of the study and areas for further research (Sections 8.5 and 8.6).

8.2 Summary of main findings and arguments

The research questions that were the focus of the discussion are:

1. What are the characteristics of fraud in the Kenyan banking industry?
2. What are the perceived characteristics of those that perpetrate fraud in the Kenyan banking industry?
3. How do banks approach fraud management?
4. Are there differences between the approaches to fraud management adopted by Kenyan and international banks?

Each of these questions can be addressed from a combination of primary research generated from both qualitative and quantitative findings and secondary research.

8.2.1 Fraud in the banking industry

The first research question addressed the characteristics of fraud in the Kenyan banking industry. The information that this question is answered by is primarily indicated in the quantitative survey and was of an exploratory nature. In general, the banking industry is highly aware of fraud, with 90% of respondents indicating that fraud is a major problem, 88.3% indicating that fraud was likely or very likely to be encountered in the banking industry, and 83.3% of respondents indicating that it was either increasing or increasing rapidly. This clearly indicates that the banking industry is highly aware of the problem of fraud and its implications for the industry. Economic pressure, advancements in technology and sophistication of criminals are seen as the main reasons behind the general increase of fraud in the banking industry but on the other hand improved control and technological measures coupled with a small improvement in the effectiveness of the justice system have mitigated the increase in fraud.

Notably, all of the banks indicated at least one incident of fraud within the past year. The average mean loss to banks within this period was around KES 21 million (USD 277,000). There was a wide variation in the amount of fraud reported, with the minimum fraud totalling KES 118,000 (USD 1,509) and the maximum fraud being around KES 271 million (USD 3,466,000). However, the majority of fraud reports were much closer to the median. Fraud for the responding banks averaged between 1% and 1.5% of annual turnover, with international banks and subsidiaries having the lowest rates of fraud and regional and local banks having the highest rates of fraud. (Of course, this does not necessarily indicate that the amounts lost are higher at local banks, since local banks, having less income, will be more susceptible to losses in terms of the per cent of turnover.)

The outcomes of this survey indicated that the majority of fraud in the Kenyan banking industry is both relatively low-volume fraud and is not technologically sophisticated. The majority of the frauds occur through misdirection, theft or appropriation of cash or cheques; only a few cases of fraud were associated with credit cards, and there was little online fraud reported, largely due to the relatively limited scale of online banking in

Kenya. The issue of technological constraints is verified by interview findings, which indicate that overall fraud that is detected is not very sophisticated. However, there is a significant concern that problems faced in fraud detection are due to lack of sophisticated fraud detection systems; the research indicated that the majority of fraud cases that were reported were in fact found by accident. Evidence indicates, however, that this is not unique to Kenyan banks, and in fact inadequate fraud controls is an issue that plagues the global banking industry. Thus, the Kenyan banking industry is probably not very different in terms of the fraud that is experienced than the global average, although there are some differences created by the level of technology used within the industry.

The majority of fraud is investigated internally due to fear of damaging the banks' reputation. Banks also have little confidence in the law enforcement bodies and the judicial system leading to a preference to negotiate and settle cases out of court, avoiding fully prosecuting the perpetrator, thereby encouraging the vice of fraud as the perpetrators know they can buy their way out. However, there is a greater tendency among the international banks to institute criminal proceedings against fraudsters as compared to local, national and regional banks. Other reasons such as the length of time involved in prosecuting perpetrators, the high acquittal rate, low recovery rate, lack of skilled and trained police, prosecutors and judges (in the area of fraud prosecution and investigation) and corruption among others have created a low appetite in the banking industry for seeking the maximum punishment of fraudsters.

The frequently employed measures used by banks in preventing fraud include improving or reviewing internal controls, training employees on fraud prevention, establishing fraud prevention policies, establishing an ethical code of conduct and screening or reference checks on new employees. The use of protective software, passwords and continuous auditing offer banks some measure of security against fraudulent activities. However, highly effective software approaches such as data mining, data sampling and digital analysis are less commonly employed by banks supporting findings by Bierstaker et al. (2006). For the future Kenyan banks need to be ready to invest in fraud detection and software approaches such as data mining, digital analysis and forensic services (forensic

auditing and forensic accountants) as these have been found to be highly effective by a minority who use them. Anti-fraud technology comes with a high price tag. However, the banks must consider the benefits of such technology which far outweighs the cost and results in effective fraud prevention and detection. Presently, as revealed by this study, fraud may be considered to be small scale fraud. This perhaps mitigates against large expenditure in anti-fraud technology. The scale of fraud is nonetheless expected to increase necessitating future investment in robust technologies.

This study has concluded that the size and/or percentage of fraud loss did not vary with the type of the bank. The study also found that fraud loss did vary with the size of the bank but not consistently. The findings therefore did not support previous studies by Murphy (1993) and Barnes and Webb (2007) possibly due to the use of a relatively smaller sample drawn from one specific industry and the differences in categorization of employee size.

There is no sufficient evidence in this study to support views (Abiola, 2009; Fisher et al, 2001) that international banks in Kenya are more likely to prosecute fraudsters and that local banks are more likely to avoid prosecuting. In addition banks are less likely to prosecute external perpetrators than internal perpetrators.

There is weak support for a number of issues regarding fraud and the type of fraud prevention method employed by the banks. However, the study reveals evidence that supports the findings by Barnes and Webb (2007) who established that there was no significant relationship between the size of fraud loss, or the susceptibility of the organisation, and the incidence of fraud or theft.

Overall, fraud is a significant concern in the banking industry, even if the loss figures are not proportionately on a very large scale. The overall loss to the banks was primarily from low-volume, technically uncomplicated frauds, and only one reported fraud posed a significant threat to the stability of the bank itself. However, the banking industry does appear to be very aware of fraud and its potential for significant growth.

8.2.2 Characteristics of perpetrators

The second research question addressed the matter of the characteristics of those that perpetrate fraud. This question was addressed from a number of different angles. From a theoretical angle, the theoretical framework considered the fraud triangle proposed by Cressey (1973), which suggested that in order to overcome social norms enough to commit a fraud, an individual needed a motivation (usually consisting of an un-shareable financial problem that cannot be resolved otherwise), the opportunity to commit the fraud, and a rationalisation that would allow for the fraud to be justified. This was then modified, in light of the technological foundation of the modern banking industry, to include technical skill and collusion, in order to allow for the individual to successfully complete the fraud. Most telling was the use of collusion in almost all cases, either with another internal party or with an external member such as a customer. These collusions tended to marry the access of one party with the requirements of another; for example, junior managers were commonly involved in fraud, as were tellers and others that had access to cash. Fraudsters were also relatively younger and male, which is consistent with empirical findings regarding fraud that have been studied in other contexts. This study has therefore identified one known dimension (capability) and one new dimension (collusion) in addition to the elements of the Fraud Triangle. This is discussed later in Section 8.4.1 of this Chapter as a part of the contribution to literature in the field of fraud.

The Fraud Triangle adequately depicts and explains the actual fraud situation within the Kenyan banking industry. The majority of respondents identified un-shareable financial problems recognized as the reason for fraudsters committing fraud, such as living beyond their means, greed and financial pressures mainly associated with individual and family problems. The act of committing fraud simply for the purposes of exploiting an opportunity, rather than meeting some form of pressure sets the Kenyan bank fraudster apart as predominantly a “predator”. The idea of a predator is pursued further in Section 8.4.2 of this chapter. Fraudsters also used the classical justifications for fraud, especially including the chance to get rich quickly, family pressure, the inability to obtain the funds elsewhere and a general atmosphere of fraud. The quantitative study suggest that

motivations such as gambling and substance abuse seem very low in the industry as did rationalization such as revenge and being underpaid.

8.2.3 Approaches to fraud management

The third research question addressed the problem of how banks tend to address the problem of fraud. In the empirical literature, fraud prevention techniques had three focuses, including external auditing, internal auditing, and mechanized approaches that relied on information technology in order to detect fraud that is occurring and prevent further fraud from occurring. The empirical literature indicated that dismissal and prosecution were the most likely outcomes for fraud.

These empirical findings in the secondary research were tested in both the qualitative and quantitative findings. The findings indicated that, in common with other banking practices, auditing and information technology formed a major portion of the fraud detection and prevention strategy. However, this was limited by the relative lack of priority given to issues of fraud. Only a relatively small portion of the banks had dedicated fraud departments or officers; instead, fraud was often investigated by ad hoc members of the management team that were appointed once fraud was found. There were also significant issues with funding for fraud prevention. In particular, many of the banks indicated that they had *no* specific budget for fraud detection and prevention, while others indicated that the fraud budget was not a stand-alone item and was included under different heads such as training, information technology, internal controls etc. The success of the fraud prevention and detection methodologies generally employed by the banks can be assessed by the way in which frauds are detected; some 33% of fraud was detected by accident or chance and 23% through the combination of internal and external whistle-blowers, while only 18% was detected through internal controls and 10% through internal audits. Thus, the institutional response to fraud, although it was consistent in form with the expectations of the researcher, did not conform in terms of the expectations of effectiveness. However, the sizeable percentage of whistle-blowers, both internal and external, indicates that this is a successful approach to creating a culture of fraud

prevention. Thus, the detection and prevention methodologies employed by the banks can be rated as being adequate.

The response to fraud is of interest, as the quantitative evidence indicated that prosecution was a relatively unpopular option compared to what might have been expected from a Western institutional context; only 47% of the cases involved investigation by law enforcement bodies and of these only 28% to 30% of internal parties were prosecuted. Prosecution rates for external parties in this study were significantly higher, at 60% to 80%). The alternative institutional option of civil prosecution was even less popular, with only 6% to 11% of internal parties and 23% to 29% of external parties being subjected to civil prosecution for recovery. In majority of internal cases, the action that was taken was simple dismissal, while in at least a third of the external cases no action was taken at all. This seemingly low rate of institutional involvement was readily explained within the qualitative interviews, when the bank representatives explained that the police in Kenya do not have significant fraud investigation capacity or skill, and the prosecution of fraud cases is lengthy, uncertain, and expensive. The respondents also pointed to a failure within the legal structure itself: there is no clear definition within the law for credit card fraud, which makes such cases difficult to prosecute. Overall, participants indicated that the expense of civil or criminal prosecution, combined with inadequate legal structures, meant that prosecution of all but the most egregious frauds was neither cost-effective nor time-effective for the bank. The preferred strategy in minor cases or cases where the party was amenable to negotiation of a settlement for reparations was to take the approach unmediated by the courts. Thus, the reluctance to prosecute on the part of the banks is demonstrated to be a business decision. A large percentage of fraud cases were not followed up by the banks in order to secure a successful prosecution.

One of the areas banks in Kenya have been found wanting in terms of internal controls was the selection and recruitment of bank staff. As indicated throughout this study, fraud is perpetrated by an individual(s). It is imperative therefore that the banks hire the right individuals as a measure towards managing fraud. Inadequate background checks at the time of recruitment have opened a door to potential serial fraudsters entering the banking

industry. Information available via the Kenya Governments' "Certificate of Good Conduct" system is not always reliable as data can be easily manipulated. There is therefore no central reliable employee reference check system that exists in the country making it difficult for the banks to secure vital information from credible sources. Yet not all the blame should be placed on a central reference system. Banks need to share part of the blame as the study has revealed that banks have hired employees with a known history of fraud and in some cases ignored credible references. Greater caution needs to be taken in staff recruitment as a step towards better fraud management.

8.2.4 Differences between Kenyan and international banks

The fourth research question asked whether Kenyan banks and international banks have different approaches to fraud management. This was tested using a combination of quantitative and qualitative techniques. There were some differences found in the results, such as the amount lost to fraud and the use of formal fraud budgets and some approaches. The interviews demonstrated that international banks are more likely than local and regional banks to be active members of the KBA, and that these banks were more active in the process of creation of a database that could help to identify fraudsters and other potentially dangerous employees. International respondents also indicated that prosecution was important, and seemed to be more likely to engage in it. However, there is the possibility that international banks may be following wider policies and are able to ignore the costs and problems arising from the legal structure in Kenya. Overall, there were differences that were associated with these banks, but the differences were often not issues of orientation toward fraud or acceptance of fraud, and nor do the differences appear to be strictly culturally based. In particular, availability of resources to fight fraud is likely to be very different between international and local banks because international banks have far more financial, technical and human resources.

8.3 Contribution to the Literature

This research project was undertaken with the understanding that the literature on the banking industry in Kenya, and in Africa generally, is relatively sparse. This research has endeavoured to provide more information on the banking industry in Kenya, providing

both quantitative findings as well as qualitative findings that serve to add more depth to the literature.

8.3.1 The role of institutions and societal structures

One of the main contributions to the literature that this research has provided is reinforcement regarding the role of institutions and societal structures in detection, prevention, and prosecution of fraud. It is often simpler, when coming from a context where there is strong respect for the rule of law and strong policing and legal institutions, to place blame on banks and other companies that do not use the court system or other legal methods to address the problem of fraud. However, as the interviews with bank management and fraud investigators revealed, the situation is not as simple as that. Simply, without the strong policing and prosecution institutions that are generally present in most Western countries, but which are noticeably lacking in Kenya, it is often a rational business decision to not prosecute for fraud rather than to prosecute for fraud, as it is both simpler and less costly to do so. This can be viewed as a contribution to the literature, because it enforces the notion that businesses must operate within an external context, and this external context is key to how these businesses will make their operating decisions and what operating decisions will be made. It also challenges the notion that African businesses are operating under substantially different business rules than are Western businesses; for example, the interviewees noted that the decision to prosecute or not to prosecute for fraud was not based in societal connections or vague notions of 'tribal solidarity,' but was instead based on rational business decision making processes. This places this research outside the scope of much business research on African institutions, but it also provides a valuable means of identifying the influence of the institutional environment on organizational decision making e.g. in prosecuting fraud cases.

Ironically, the above discussion in this section may explain why international banks that originate from countries with stronger laws are more likely to take some form of action against fraudsters and show better defences than domestic banks.

8.3.2 Information on regulation and treatment of fraud

A second contribution to literature is that this research provides information regarding regulation, treatment, and detection of fraud in Kenyan banking institutions. This is an area that has been relatively little explored in the academic literature, with the majority of reports that were found stemming from international non-governmental institutions such as the World Bank or IMF, or Government sources such as the Central Bank of Kenya. This general lack of information regarding the banking industry in Kenya along with other Sub-Saharan African countries means there is relatively little information for organisations and companies in Kenya and outside it. Given that the strength of institutions is one of the major factors in market entry, it is likely that the state of the Kenyan police and court institutions may prove to be prohibitive to entry for some firms. However, the provision of material regarding the nature and scope of fraud in the Kenyan banking system also provides some guidance for firms that are hoping to enter this market. Thus, this could be useful for practice as well.

8.4 Contribution to theory

This study has made some significant contributions to fraud theory based on the nature of fraud in Kenya's banking industry as well as making some contribution to the conceptualization of fraud.

8.4.1 The Fraud Pentagon

An important contribution of this research is to confirm the value of the Fraud Triangle as a theoretical framework for understanding of fraud. Previous research has shown that the Fraud Triangle framework is useful for analysis of fraud cross-culturally, and it has been used in a number of empirical studies that have considered the problem of fraud from many different cultures. The Fraud Triangle was just as successful in describing motivation, justification, and opportunity to commit fraud in the Kenyan banking context as it has been in American, British, European, and Asian contexts. This indicates two issues of importance. First, the Fraud Triangle's robustness as a theory of fraud has been reconfirmed in that the three elements suggested by Cressey (1973) were found to be present in the frauds considered in this study. Second, this demonstrates that there is in

fact nothing culturally unique about the practice of fraud in Kenya; instead, motivations, justifications, and opportunities are all very similar in origin. The main difference in fraud and its treatment did not appear to be in the fraud itself, but in whether or not the fraud was addressed through official institutions or not. This study did not reveal that Kenya was unique in terms of the types of fraud based in the literature.

Another implication is additional factors in the commission of fraud. The modern banking environment requires technical skills or capability, expanding into the fraud diamond (Wolfe & Hermanson, 2004). This research has confirmed that the persons involved in fraud held positions within the organization where they could exercise their technical skills and capabilities to assist them in carrying out fraud. Thus this study has adopted the element of capability as a factor in the commission of fraud. This study noted that collusion is also a major concern of fraud in Kenyan banks and an element worth considering when it comes to the individual factors. A further suggestion is now made within this study to include collusion as a key element of fraud in as far as Kenyan banks are concerned bringing the number of significant fraud elements identified in this study to five – pressure, opportunity, rationalization, capability and collusion. Given the impetus that capability adds to the dimension of fraud and the idea that the new dimension, collusion, can be viewed as a stand-alone variable these two can be integrated along with the other variables of the fraud triangle into a new conceptualization of fraud called the "Fraud Pentagon" (Figure 8.1). The fraud pentagon suggests that in Kenya's banking industry the combination of pressure and opportunity on the individual, when rationalized and coupled with the technical skills and capability of one or more than one person working in collusion, may lead to fraud.

More importantly, this study has contributed a new dimension in that the analysis has helped to move the study away from a criminology/sociological focus on individuals and their motivations to a more business or organizational focus that emphasizes on other linkages such as collusion and contexts such as the legal structures and other business environmental factors (discussed further in Section 8.4.3). Therefore dealing with fraud within the banking organizations requires multi-thronged strategies that can address the

characteristics of the individual perpetrator, competition, industry co-operation, legal structures and collusion among other factors.

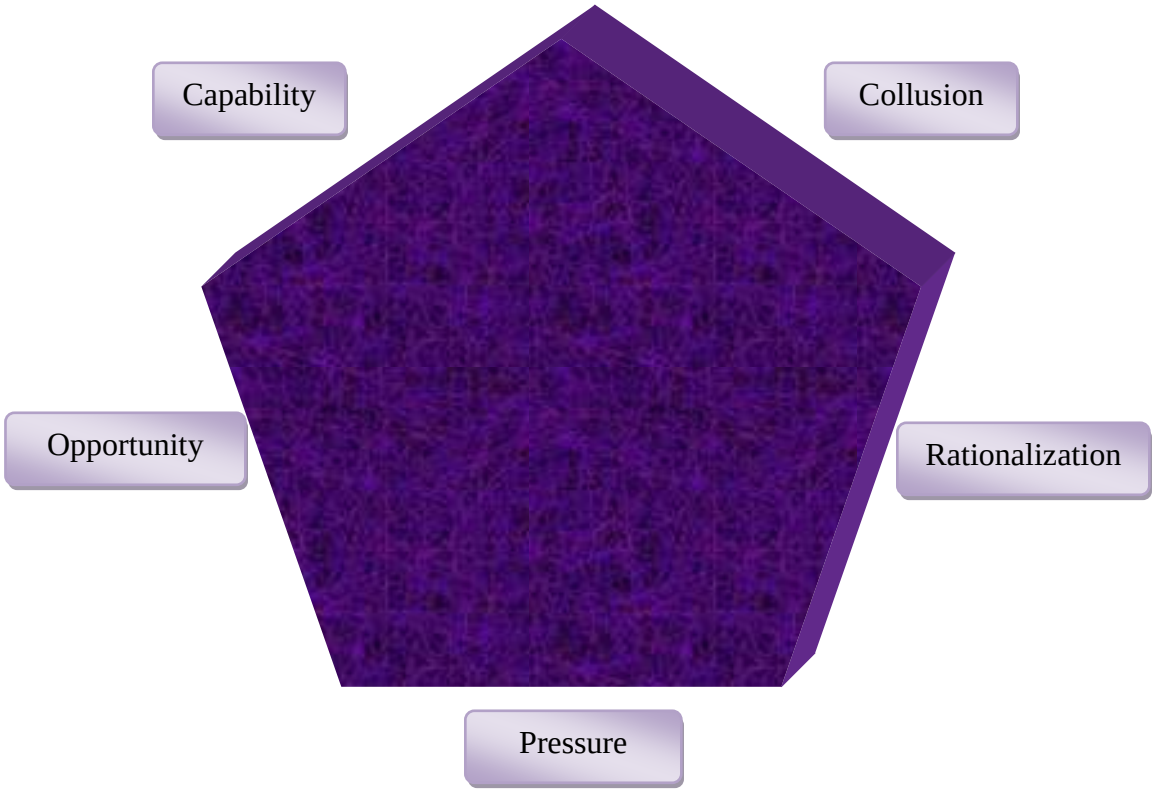


Figure 8.1 The Fraud Pentagon - a proposed model of fraud in Kenyan banking

This model builds on the Fraud Triangle (Cressey, 1973) and Fraud Diamond (Wolfe and Hermanson, 2004), incorporating collusion, a predominant theme of this study. The researcher hopes that this model can be applied to other banking contexts, allowing for greater understanding of fraud as a social as well as an individual phenomenon.

8.4.2 Opportunity and the Predator

The Fraud Triangle presumes the existence of pressure, opportunity and rationalization. In this study, opportunity rather than pressure was perceived to take the lead. This is an important contribution as it implies that most of the bank fraudsters are predators and not the accidental fraudster (Dorminey et al., 2010). The predator as defined in Chapter 2 (Section 2.3.2.6) is an individual whom right from the onset are inclined or disposed to defrauding the organization. They develop intentional fraud schemes unlike the accidental fraudster who does not set out to commit fraud but is lured gradually before they commit their first fraud. This has implications on the way the Fraud Triangle is applied as it may not fully fit the description of a predator but it has been tailored to suit the accidental fraudster (Dorminey et al., 2010).

8.4.3 Conceptual framework

The initial conceptual framework of this research took into account three broad aspects that impact on or encourage the incidence of fraud. Individual characteristics were based on the fraud triangle, while the bank and the industry were described with internal industry factors. External factors described the general environment. However, the findings suggest a variation on the initial conceptual framework (Section 3.10).

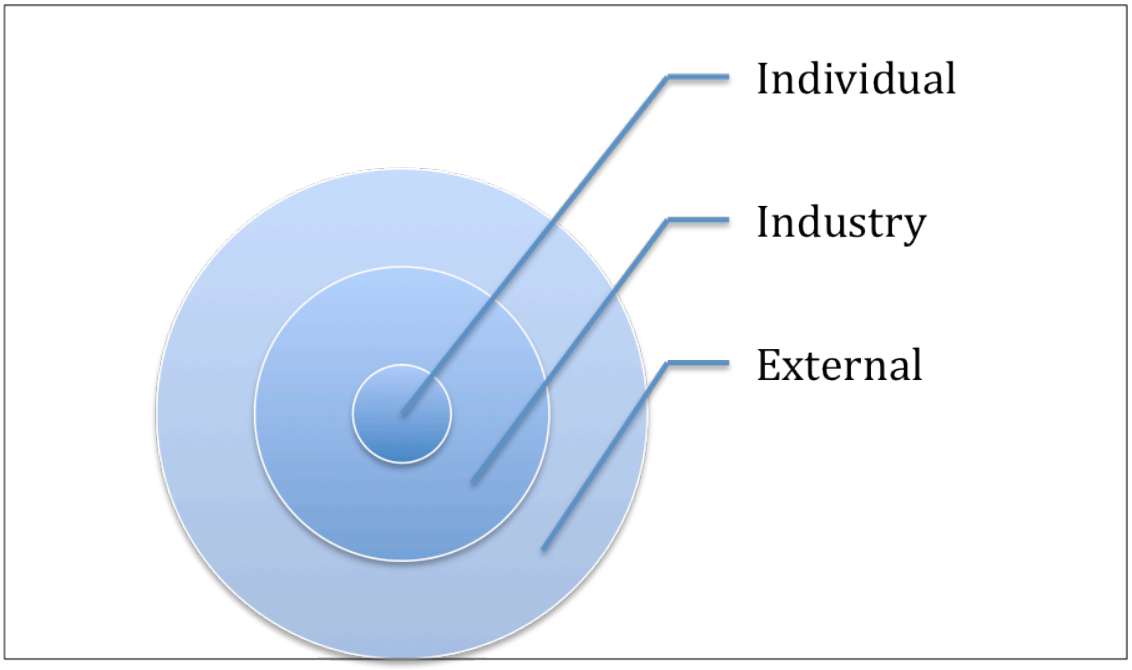


Figure 8.2 Levels of revised conceptual framework

In Figure 8.2 a single model is constructed that reflects all three levels of the revised conceptual framework. However, instead of viewing the conceptual framework as being composed of *three separate distinct components* as originally done, the suggested conceptual framework consists of *three levels* that are distinct yet interlocked or inter-dependent. Figure 8.3 presents the revised framework.

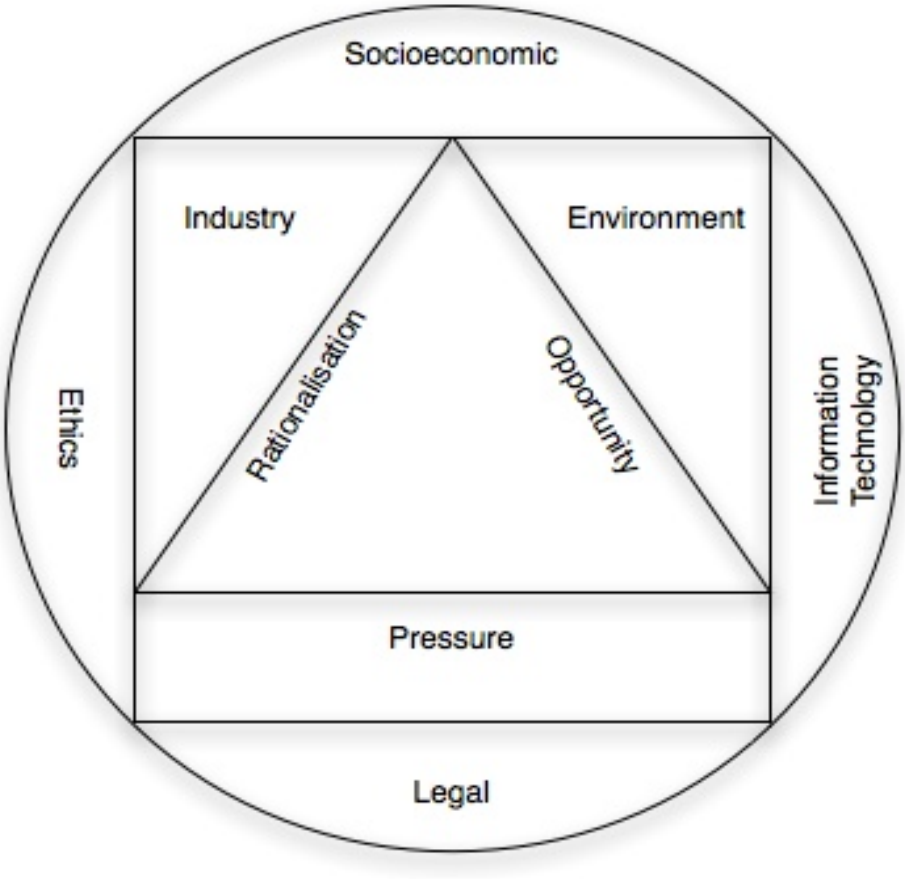


Figure 8.3 Emergent conceptual framework

This framework continues to place the individual at the centre of the fraud, enveloped by the internal bank and industry environment and then by the external environment. This acknowledges that while individuals are responsible for fraud, capability, rationalization, and other factors are influenced by the banking industry structure and environment, including socioeconomic conditions and institutions. It also reflects the influences on individuals to commit fraud and the effects of the individual and industry conditions on

the banking industry, visually demonstrating the shift from individual criminological theories of fraud to broader theories of organizational fraud which introduces linkages and contexts such as industry and external factors and emphasizing social and cultural issues (expressed in Section 8.4.1). The conceptual framework that finally arises from this study is therefore a contribution to the theoretical and conceptual framework of banking in Kenya with the possibility of the same being extended or generalized to other bank settings.

8.5 Policy implications

The discussion of the findings have generated a number of recommendations for Kenyan banks, as well as for general reform of the Kenyan banking and legal system in order to reduce the potential for fraud within the system. These findings have been used to generate a set of recommendations for banks and for policymakers as well as the KBA to improve conditions in the banking system.

8.5.1 Policy implications for Banks

There were some recommendations for individual banks that have emerged from this study. These recommendations are based on the outcomes of the research combined with insights from the literature.

First, the banks should pay attention to online banking fraud because as the study has shown the changing competitive environment means that it will soon become significant as banks begin to introduce online banking to all its customers in the near term. Mechanisms should be in place to prevent online fraud before systems are implemented, already a problem with banks that report a high rate of customer-based fraud with implemented systems. Based on literature, issues like online credit and debit card fraud, which is committed by people associated with the bank (Moore, Clayton, & Anderson, 2009), also needs to be considered. This fraud is unlikely to be caught by existing systems. Banks need to consider their security levels on external IT systems, as these systems are likely to come under attack from the outside and may result in significant losses. Banks in Kenya, either individually or jointly under the KBA, could look at best

practice of other banks worldwide to learn how they have tackled similar fraud and so perhaps exploit the benefits of internet adoption.

A second recommendation is a strategic recommendation regarding the way that banks consider fraud. In many cases, responses in this study indicated that fraud was considered to be a one-time or sporadic loss, and so it was not worth assigning routine resources or staff members to deal with the problem. However, banks also reported multiple, repeated 'sporadic' losses. This indicates that this is not a short-term problem or a rare occurrence, but a routine occurrence that should be considered in a more strategic light. Changing the orientation of thought about fraud from a consideration of the problem as a rare occurrence to thinking about it as a common risk would change the understanding of fraud in the banks and possibly improve the bank's ability to be proactive and reactive to the occurrence of fraud.

Anti-fraud policies should be applied in the context of wider business strategies. This study has highlighted how the security dimensions of the "Know Your Customer" (KYC) policies are being undermined by marketing and competitive considerations. It has also shown above how competitive pressures may encourage Internet banking adoption before security systems are fully prepared as found in the research. This will no doubt lead to an increase in fraud risk. Such compromises suggest the need for an inter-strategy co-ordination or a multi-thronged approach to strategy. Again this lends to the contribution that this study has moved away from an individual focus on fraud to a more organisational focus.

8.5.2 Policy implications for the KBA

There are four main recommendations that have emerged from this research for the Kenya Bankers Association (KBA), addressing guidance and improved customer awareness, information sharing, international ties, and legal institutions.

The first issue is that of customer awareness campaigns. Banks are reluctant to engage with customer awareness campaigns about fraud, although they are known to be

effective, because of the potential for reputation loss. Considering that brand identity is key to maintaining customer loyalty in the banking industry (Sweeney & Swait, 2008), and that the banking industry in Kenya is crowded with over 40 banks offering customers ample choice, this is unlikely to change. However, the KBA, as a banking association connected with all banks, is well-placed to conduct such a campaign. The KBA should take on a role in customer education, producing materials to be disseminated through all member banks regarding the potential for fraud, how to detect it, and how to report it. This could substantially improve coverage of the early-warning system of customer awareness without placing the brand reputation of any particular bank at risk.

The second issue concerns the urgent creation of a centralised fraud database. The centralization of peoples' identity in a national database system will go a long way in the establishment of a fraud management system, strengthen the investigative capacity of the Bank Fraud Investigations Department (BFID) of the Central Bank of Kenya and enhance judicial prosecution or consequences of financial fraud.

The third recommendation focuses on international fraud issues. The KBA has an affiliate role with international banking associations. These connections could help to improve international fraud detection capabilities and help to leverage international fraud detection knowledge and practice for use in the Kenyan banking system. The KBA should create strategic partnerships between banking associations in other countries and the KBA, allowing for access to technical knowledge as well as formation of network relationships that could benefit the Kenyan banking industry as a whole. Dahan et al. (2010) confirm that similar partnerships have been formed between multinational enterprises and non-governmental organisations in the region in order to improve technology and knowledge transfer as well as improve regional commerce. Other literature shows that this approach could be modified in order to allow for cooperation by business associations, in order to reap some of the same benefits (Sweeney & Swait, 2008). The same structure could be therefore be used to promote knowledge diffusion from international banks throughout the industry. This approach would allow for smaller

banks to begin to develop increased technical expertise, as well as to bring them more firmly into the KBA organisation.

A fourth recommendation in this region is to use the KBA's political 'clout' to improve the judicial and legal handling of the issue of bank fraud. Special concerns include lack of formal credit card laws, slowness of change, and out-dated and antiquated banking fraud laws. Organisations like the KBA have power to change these conditions using direct influence on the government through lobbying activities and public awareness and motivation of the public to change these laws (Bernhagen & Bräuninger, 2005). By applying this power and by providing its expertise to the Kenyan government, which respondents characterised as substantially overloaded and lacking the necessary expertise to implement these types of reforms, it would be possible for the KBA to improve conditions in terms of judicial and legal treatment of fraud. This would be a highly appropriate use of industry power that would benefit the full industry, as well as improving conditions in society overall.

As an apex body in the industry KBA can also potentially take on the role of an educator for police and prosecutors. Seminars and workshops should not only be directed to the internal needs of the banks and customers but also embrace those who work with the industry to prosecute fraud cases. By so doing they will improve legal skills and reduce the number of cases acquitted by the courts due to inadequate evidence and poor legal skills.

8.5.3 Policy implications for the Kenyan Legal System

The recent enactment of the Anti-Money Laundering Law in December 2009 and the establishment of Credit Reference Bureaus in 2009 will help to boost the banking industry's fight against fraud. However, it is clear that the Kenyan legal system must undergo some structural reforms in order to increase the robustness of the Kenyan banking system towards fraud. Although banking fraud is not considered to be a significant problem at this time, the evidence indicates that this will become an increasing problem over time. For example, drawing from literature, telecoms fraud (of which some

banking fraud is a subset) resulted in a loss of $700 million in Africa in 2009 (Ghosh, 2010). These figures are only expected to increase over time. This is particularly problematic with the growth of mobile banking services, which are highly popular in Kenya and Africa on the whole as a means of providing non-branch banking services. Frimpong (2007) notes that the potential for banking fraud is often seen as one of the factors that put small and medium enterprises (SMEs) off the idea of online banking, reducing the uptake of internet banking even in cases where this could be a possible improvement over existing banking services. Finally, there is the potential that advance fee fraud, (often called '419' fraud) originating from Nigeria, could affect the Kenyan banking system's overall reputation. The last issue is in many ways the most serious issue, as it has been shown to affect the investor confidence in other countries, reducing the country's ability to compete in terms of foreign direct investment (FDI) and economic development (Ampratwum, 2009). Thus, it is clear that the government *must* act to reduce the structural barriers to prosecution and improve access to the judicial system for banks hoping to reduce fraud levels.

Based on the findings of this research the suggested ways for improving the judicial and legal system is a combination of restructuring the laws and judicial system and advanced training for police, attorneys, and judges in issues of banking fraud and other financial crimes. The Central Bank of Kenya already has a dedicated police unit (the Banking Fraud Investigations Department - BFID) devoted to the prosecution of financial crime, according to the interviewees. However, this capacity should be expanded in order to allow for improved support from this region. Another possibility is advanced training for a larger number of police officers and others through a financial crimes training program. These types of programs are one of the ways in which police units in other regions have been able to keep up with financial crimes and have gained an increased level of ability to combat these crimes (Michel, 2008). Other alternative measures include increased organisational ties with international agencies such as Interpol and other national policing agencies from regions that have achieved some degree of success with international banking crime (Michel, 2008). Consistency in the police force that prosecutes fraud at the BFID must be established. The regular changes made in the police force deployed at the

BFID makes it difficult for fraud cases to be followed up to a successful conclusion. Perhaps instituting a minimum serving term for police within the department can bring stability to this department and enhance its efficiency and effectiveness in managing and reducing general levels of fraud within the banking industry.

Finally, as revealed from this study, the court system must be improved in terms of the time and cost involved in fraud prosecution, in order to increase the likelihood that banks will choose to use prosecution as a means of deterring financial fraud. Although these measures may not seem important at this time, as bank officers estimate that the losses to fraud are relatively low, they are only likely to grow more substantial over time especially in increasingly global financial markets and as evidenced by recent press reports highlighting the reported fraud losses in the previous chapter. The likelihood of non-prosecution also encourages fraudsters to engage in fraudulent acts. Making changes to the judicial and policing system now will prevent this excessive growth over time.

8.6 Limitations of this study

This study has provided a comprehensive view into the treatment of fraud within the Kenyan banking system. Nonetheless there are some potential limitations that should be considered in the discussion of these results and consideration of the outcomes of the study.

8.6.1 Generalizations

First, the results are geographically and temporally limited. Although they provide an insight into the Kenyan banking system (and indirectly, into structural conditions of the industry and of judicial and political systems in place at this time), they cannot be applied to any other countries except in terms of the general findings and lessons learned. These results, in other words, apply only to Kenya on the large scale. Furthermore, they are *temporally* limited – that is, the conditions in place now are described, and some historical information is included, but this does not imply anything about conditions that may take place following changes to industry, government, technological or the banking

structure. This should be considered in terms of the application of the findings of the study to other contexts or over a long period of time.

8.6.2 Validity of data

Small samples are often considered to be 'non-representative' resulting in generalisations that could be used subjectively by the reader. The sample sizes used in this study was not large but every effort was made to ensure its representativeness. In order to achieve representativeness respondents were drawn from a cross-section of local, national, regional and international banks. Respondents were chosen using purposive and snowball sampling. Purposive sampling allows for the selection of specific groups in the sample and in so doing obtain a representative sample. The key informants in this study were specifically chosen as they are the bank staffs who are specialists in the area of fraud and were considered to be the best informed in the organization on fraud matters. Though the sample size appears to be small (17 for interviews and 60 for the survey), it is representative of the 40 banks that were the population of the study as representativeness has more to do with where the sample is drawn from rather than with the sample size. It can be argued that the views of a few people may not adequately capture an entire organizations view. Selecting informants who directly oversee the functions responsible for fighting fraud helps to mitigate the limitation of representativeness. Therefore it could be safe to assume that the views expressed by two or three respondents in the qualitative interviews could be fairly sufficient in representing the banks' perceptions, views and attitudes towards fraud as these respondents are the experts in the organization.

Nonetheless it is important to acknowledge that the sample size used in the quantitative study could influence the outcome and precision of the statistical inferences obtained from using the Chi-Square test. In future and, with the benefit of hindsight, a repeat of this or a similar study using a larger sample size may return different results. Therefore the results and claims of the hypotheses testing should be used conservatively.

8.6.3 Respondent bias

A second limitation in these results must also be considered. That limitation is the potential for internal respondent bias. They could also have been some unintentional respondent bias of some areas of fraud not being detected. As noted above, there are some instances where respondents felt it would be unwise to disclose, or did not truly know, the full scope of the fraud issue. Given this, and given the importance of brand reputation in maintaining customers, it is possible that some respondents have withheld information that would change the interpretation of the findings, or that they did not have access to this information in the first place. For example, information regarding specific fraud prevention technologies may be limited, or there may be limitation of the scale and scope of fraudulent activities within the organisation itself. These are issues that could lead to respondent bias, through the hiding of potentially important information that would change the outcomes of the study if it were revealed. Although the researcher tried to avoid this potential both by cross-checking information between sources and by reassuring participants that the information regarding their situation would not be disclosed, this remains a potential issue within the results of the study. If this *is* the case, it is likely that the outcome of this bias would be to provide an overly optimistic or reductive view of fraud in the Kenyan banking system, as participants would not want to provide the potential impression that fraud was more widespread than it actually is. Thus, there is the potential that this research is overly optimistic in terms of the estimation of fraud amounts, although it is not anticipated that there is substantial overestimation of the effectiveness of fraud measures or other such issues. The researcher did not explicitly detect this bias as the responses from participants showed consistency; but nonetheless it is best if the potential for this bias is acknowledged rather than ignored as there is a risk in researching the 'policeman' as it could lead to biased views from the respondents.

8.6.4 Perceptions

A third limitation to this study is that it raises issues regarding the perceptions of the respondents and perceptions of fraudsters' motives. The study does not highlight what the fraudsters actually think or do. However, the information coming from the respondents who are fraud fighters may be more credible than information raised from the fraudsters.

But again there is scope for bias here in the interests of those combatting fraud to portray the fraud challenge as difficult, costly etc.

8.6.5 Gaining Access

Gaining access to respondents is a critical part of gathering information for research. Fraud is a sensitive topic not only within Kenya's banking industry but also in other industries. Organisations and individual respondents tend to view the researcher as an "investigator" and still treat researchers with great suspicion. Though the researcher found the respondents in the banking industry more open than has traditionally been the expectation in Kenya, there was a sense in which the respondents held back on information and others refused out-rightly to participate in the study. In some instances respondents held back on some information with claims such as they were bound by Codes of Secrecy. As a result this topic was toned down following the pilot study and some pertinent questions that pertained to specific aspects of fraud were not included in the research. Gaining access was not very easy but through snowball sampling a network of respondents was finally established through personal contacts and friends. In the end the sample was large enough with at least thirty out of a possible 40 banks participating. Considering that many countries have far fewer banks this research was able to achieve much by reaching at least 75% of the banking institutions. Thus in spite of the problems associated with access the findings of this study can be used to make limited generalizations.

8.6.6 Theoretical limitations

One of the main limitations that this study faced is the lack of theoretical frameworks that can be used to discuss fraud in the local context where politics and government are the main contributors to large scale fraud. As discussed in Chapter Two, the main cases of fraud in the banking industry in Kenya have been politically motivated and the history of fraud has roots in political connections. There is also lack of adequate literature in regard to fraud in Kenya and Africa. This coupled with limited or selected release of information from the respondents made it impossible to fully explore fraud using existing theoretical frameworks.

8.7 Areas for Further Research

This research has provided a great deal of information regarding the Kenyan banking system and the management of fraud within this system. However, as always, there remain areas for further research that could be exploited. A number of potential areas for further research are identified and the ways in which this research could be conducted are discussed.

One area for further research is into customer awareness of banking fraud. The research highlighted an interesting contradiction – much fraud in the banking system is actually detected by customers that notice something amiss with their bank accounts. However, there is little attention paid to building customer awareness for the potential for fraud. On the one hand, this is understandable, given that banks do not want to lend the impression that they are vulnerable to fraud, leading customers to potentially abandon them for banks that do not lend this impression. (Of course, the difference in the potential for fraud would not be related to the actual reduction in fraud potential, but simply in the level of information provided to customers.) However, given that customers are a major point of awareness regarding fraud, training them to identify fraudulent activity in their accounts could greatly increase the fraud detection capabilities and robustness of the existing system. In order to do this effectively, however, it is necessary to understand what customers already know about banking fraud and fraud detection in order to design this type of informational campaign effectively. A proposed area of research is therefore in Kenyan banking customer populations, to identify the general level of knowledge regarding the issue of banking fraud and bank fraud identification. The proposed method for this research is a large-scale survey covering major geographic areas and ensuring that customers of all Kenyan banks are included.

A second area of research is more intensive research into the issue of international fraud. Most of the respondents to the interviews indicated that international fraud was a growing area of concern, and that it was simultaneously very difficult to manage due to problems with jurisdictional arrangements, lack of cooperation between international bodies, and

lack of clear laws in Kenya in some cases reducing the effectiveness of international prosecution of banking fraud. A more in-depth study focusing directly on international banking fraud in Kenya could provide insight into the scope of this problem and identify how this problem could potentially be rectified, or at least offer a way to reduce the severity of challenges that are posed by the growing internationalization of the banking sector. This research may most effectively be undertaken by extensive documentation research, including bank records and records of international agencies, judicial and legislative documentation, and all other areas concerning the issue of international fraud detection and prevention. This research would be large in scale and require substantial access to the documentation of numerous organisations; as such, it may be research that is most effectively performed outside the academic area, by a policy setting body within Kenya itself. Legal research into fraud may also be an area worth exploiting.

A third area of research can be aimed at promoting connections between international banks and local banks. It is clear that collaboration between banks is the key to ensuring that there is a reduced level of fraud within the Kenyan banking system as a whole. In particular, this research indicated that there was a consistent overlap in bank workers, which often allowed a worker or customer that perpetrated fraud in one bank to move on to another bank undetected. This is particularly important given the relative scarcity of resources in the Kenyan judicial system to combat banking fraud, so it represents a way for banks to cooperate and increase their ability to detect the potential for fraud and to avoid it. The KBA provides the obvious institutional location for establishment of a clearing house for information regarding workers and customers, which would allow banks to avoid this type of repeated fraud. Some evidence indicates that the KBA is already beginning to develop a central database for information regarding fraud both of staff and external fraudsters. However, smaller banks reported that they did not gain as much information from the KBA as larger banks, as they were less integrated into the structure. An action research project aimed at developing this database and ensuring that smaller banks have access to, and skills to use, the database would be beneficial to increasing the ability of the Kenyan banking system as a whole to react effectively to incidences of fraud. Thus, the suggested research project is to implement a database that

can be used by all banks and to assist banks in development of interfaces and methods for use of this system.

Bibliography

Abdolmohammadi, M. J., & Owhoso, V. D. (2000). Auditors' ethical sensitivity and the assessment of the likelihood of fraud. *Managerial Finance, 26*, 21-34

Abiola, I. (2009). An assessment of fraud and its management in Nigerian commercial banks. *European Journal of Social Sciences, 10 (4),* 628-640

Adams, M. B. (1994). The agency theory and the internal audit. *Managerial Accounting Journal, 9 (8),* 8-12

Adams, R. (2010). Prevent, protect, pursue - a paradigm for preventing fraud. *Computer Fraud and Security, 7,* 5-11

Adeleye, B. C., Annasingh, F., & Nunes, M. B. (2004). Risk management practices in IS outsourcing: an investigation into commercial banks in Nigeria. *International Journal of Information Management, 24,* 167-180

Africa Banking & Finance Conference (2010). KBA Profile: Profile of the Kenya Bankers Association. Available at: http://www.aidembs.com/banking_conference/index.php?option=com_content&view=article&id=58&Itemid=69 [Accessed on 2 Jan 2011]

Aguilar, M., Gill, J., & Pino, L. (2000). *Preventing fraud and corruption in World Bank projects: A guide for staff.* Available at: http://www1.worldbank.org/publicsector/anticorrupt/fraudguide.pdf [Accessed on 3 March 2011]

Akers, R.L. (2004). *Criminology Theories: Introduction, Evaluation and Application*. 4th Ed. Los Angeles: Roxbury Publishing.

Akers, R.L. (1996). Is differential association/social learning cultural deviance theory? *Criminology, 34 (2),* 229–247.

Aladwani, A.M. (2001). Online banking: a field study of drivers, development challenges and expectations. *International Journal of Information and Management, 2 (1),* 213-225.

Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2004). Fraud and corporate executives: Agency, stewardship, and broken trust. *Journal of Forensic Accounting, V*, 109-130.

Albrecht, S., Howe K., & Romney, M. (1983). *Deterring Fraud: The Internal Auditor's Perspective.* Altamonte Springs, FL: The Institute of Internal Auditor's Research Foundation)

Albrecht, S., and Albrecht, C. (2004). *Fraud examination and prevention*. Ohio: Thomson South Western

Alleyne, P., & Howard, M. (2005). An exploratory study of auditors' responsibility for fraud detection in Barbados. *Managerial Auditing Journal, 20*, 284-303

American Institute of Certified Public Accountants (AICPA). (2002). Statement on Auditing Standards No.99: Consideration of Fraud in a Financial Statement Audit. New York: AICPA

American Institute of Certified Public Accountants (AICPA). (2012). Fraud Prevention. Available at: http://www.aicpa.org/interestareas/forensicandvaluation/resources/fraudpreventiondetectionresponse/pages/fraud%20prevention.aspx?action=print [Accessed on 15 May 2012]

Ampratwum, E. F. (2009). Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA. *Journal of Financial Crime, 16 (1),* 67-79

Anon. (2008). Kenyan banks demand fair play. IT News Africa [online], 13 October, 2008. Available at http://www.itnewsafrica.com/2008/10/kenyan-banks-demand-fair-play/ [Accessed on 27 September 2010]

Anadarajan, A., & Kleinman, G. (2011). The impact of cognitive biases on fraudulent behaviour: the Leeson case. *International Journal of Behavioural Accounting and Finance, 2* (1), 40-55.

Anderson, D. M. (2002). Vigilantes, violence and the politics of public order in Kenya. *African Affairs, 101*, 531-555.

Arnfield, R. (2004). Banking on Digital Certificates to Prevent UK Payment Fraud. *InfoSecurity Today, May/June*, 16-18

Arnold, P. J., & Sikka, P. (2001). Globalization and the state-profession relationship: The case of the Bank of Credit and Commerce International. *Accounting, Organisations and Society, 26*, 475-489

Arun, T. (2005). Regulating for development: The case of microfinance. *The Quarterly Review of Economics and Finance, 45*, 346-357

Arun, T.G., and Turner, J.D. (2002). Public Sector Banks in India: Rationale and Pre-requisites for Reform. Annals of Public and Cooperative Economics 73(1)

Asiedu, E. (2006). Foreign Direct Investment in Africa: The Role of Natural Resources, Market Size, Government Policy, Institutions and Political Instability. *The World Economy, 29 (1)*, 63-77

Association of Certified Fraud Examiners (ACFE) (n.d.). Small Business Fraud Prevention Manual. Available at: http://www.acfe.com/documents/smallbusinessfraudexcerpt.pdf [Accessed on 30 January 2011]

Association of Certified Fraud Examiners Inc. (ACFE) (2002). Report to the Nation on Occupational fraud and abuse

Association of Certified Fraud Examiners Inc. (ACFE) (2004). Report to the Nation on Occupational fraud and abuse

Association of Certified Fraud Examiners Inc. (ACFE) (2006). Report to the Nation on Occupational fraud and abuse

Association of Certified Fraud Examiners Inc. (ACFE) (2008). Report to the Nation on Occupational fraud and abuse

Bakre, O. (2007). The unethical practices of accountants and auditors and the compromising stance of professional bodies in the corporate world: Evidence from Corporate Nigeria. *Accounting Forum, 31*, 277-303

Balancing Act. (2010). *Lack of security fears slows uptake of e-commerce in Kenya*. Issue No.185. Available at: http://www.balancingact-africa.com/news/en/issue-no-185/web-and-mobile-data/lack-of-security-fea/en [Accessed on 11 October 2010]

Baloyi, N. T. (2005). Misuse intrusion architecture: Prevent, detect, monitor and recover employee fraud. *ISSA 2005 New Knowledge Today Conference.* Sandton, SA: ISSA

Bandura, A. (1997). *Social Learning Theory*. Prentice Hall: Englewood Cliffs

Bank Supervision Report, 2006. Annual Report, Central Bank of Kenya

Bank Supervision Report, 2007. Annual Report, Central Bank of Kenya

Bank Supervision Report, 2008. Annual Report, Central Bank of Kenya

Bank Supervision Report, 2009. Annual Report, Central Bank of Kenya

Bank Supervision report, 2010. Annual Report, Central Bank of Kenya

Banking Fraud Report Shocker (2010). Kenya Television Network, Standard Group Kenya. Cynthia Nyamai, 20 September 2010. [Available at: http://www.youtube.com/watch?v=Ao-A9dB44IM [Accessed on 29 September 2010]

Barako, D. G., Hancock, P., & Izan, H. Y. (2006). Factors influencing voluntary corporate disclosure by Kenyan companies. *Corporate Governance: An International Review, 14* (2), 107-125.

Barker, T. S., & Cobb, S. L. (1999). A survey of ethics and cultural dimensions of MNCs. Competitiveness Review, 9 (2), 11-18.

Barnes, P. & Webb, J. (2007) Organisational Susceptibility to Fraud and theft, Organisational Size and the Effectiveness of Management Controls: Some UK evidence. *Managerial and decision economics, 28,* 181-193

Barth, J. R., Lin, C., Lin, P., & Song, F. M. (2009). Corruption in bank lending to firms: Cross-country micro evidence on the beneficial role of competition and information sharing. *Journal of Financial Economics, 91 (3),* 361-388

Baucus, M. S., & Near, J. P. (1991). Can illegal corporate behaviour be predicted? An event history analysis. *Academy of Management Journal, 34 (1),* 9– 36.

Bauerle, J. F. (2004). The emperor's new clothes? Benefits and pitfalls of pattern recognition software in electronic financial services. *The Banking Law Journal, 131 (7),* 656

Beasley, M. S. (1996). An Empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud. *The Accounting Review*, *71* (4), 443-465.

Beck, T., Cull, R., & Jerome, A. (2005). Bank privatization and performance: evidence from Nigeria. *Journal of Banking and Finance, 29*, 2355-2379

Beck, T., Demirguc-Kunt, A., & Levine, R. (2006). Bank supervision and corruption and lending. *Journal of Monetary Economics, 53,* 2131-2163.

Beck, T & Fuchs, M. (2004). Structural Issues in the Kenyan Financial System: Improving Competition and Access. World Bank Policy Research Working Paper 3363. Available at: http://www-wds.worldbank.org/servlet/WDSContentServer/WDSP/IB/2004/07/30/000090341_20040730101641/additional/104504322_20041117161008.pdf. [Accessed on 30 June 2011]

Benson, M.L., & Moore, E. (1992). Are white collar and common offenders the same? An empirical and theoretical critique of a recently proposed general theory of crime. *Journal of Research in Crime and Delinquency, 29: 251-272*

Benston, G. J. (1994). International harmonization of banking regulations and cooperation among national regulators: An assessment. *Journal of Financial Services Research*, *8* (3), 205-255.

Berger, A. N., Miller, N. H., Peterson, M. A., Rajan, R. G., & Stein, J. C. (2005). Does function follow organisational form? Evidence from the lending practices of large and small banks. *Journal of Financial Economics, 76 (2),* 237-269.

Bernhagen, P., & Bräuninger, T. (2005). Structural Power and Public Policy: A Signaling Model of Business Lobbying in Democratic Capitalism. *Political Studies, 53 (1),* 43-64.

Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security, 15 (5),* 529-560.

Bielski, K. (2004). Keeping Check Fraud in Check: Recent Report Looks at the Marketplace of Fraud Prevention. *ABA Banking Journal, 96.*

Bierstaker, J. L., Brody, R. G., & Pacini, C. (2006). : Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Accounting Journal, 21 (5),* 520-535.

Bigsten, A., Isaksson, A., Söderbom, M., Collier, P., Zeufack, A., Dercon, S., et al. (2000). Rates of Return on Physical and Human Capital in Africa's Manufacturing Sector. *Economic Development and Cultural Change, 48* (4), 801-827.

Bird, M. (1994). 'Combining quantitative and qualitative methods: a case study of the implementation of the open college policy' in J. Brannen (Ed.) *Mixing methods: qualitative and quantitative research.* Ashgate Publishing Limited, England Pgs. 127-143

Black, S. S., & Geletkanycz, M. A. (2006). The New Breed of Black South African Senior Managers: Helping South African Businesses Meet the Challenge of a Transforming Economy . *Organisational Management Journal, 3,* 94-114.

Black, W. K. (2005a). "Control frauds" as financial superpredators: How "pathogens" make financial markets inefficient. *The Journal of Socio-Economics, 34,* 734-755.

Black, W. K. (2005b). The best way to rob a bank is to own one: How corporate executives and politicians looted the S&L industry. Austin, TX: University of Texas Press.

Blass, A. A., & Grossman, R. S. (1996). Financial fraud and banking stability: The Israeli bank crisis of 1983 and trial of 1990. *International Review of Law and Economics, 16,* 461-472.

Blumberg, B., Cooper, D.R. and Schindler, P.S. (2005), *Business Research Methods*. Maidenhead: McGraw Hill

Blumer, H. (1969) *Symbolic interactionism: perspective and method*, Englewood Cliffs: Prentice Hall

Bologna, J., and Lindquist, R. (1995). *Fraud auditing and forensic accounting: new tools and techniques*. 2nd edition. London: John Wiley and Sons.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud prevention: A review. *Statistical Science, 17 (31),* 235-255.

Bonoma, T. V. (1985). The Marketing Edge: Making Strategies Work. New York: Free.

Bostan, I. (2010). The role of internal audit in optimization of corporate governance at the groups of companies. *Theoretical and Applied Economics, XVII (2),* 89-110.

Boynton, W., Johnson, R. & Kell, W. (2005). *Assurance and the integrity of financial reporting*. 8th edition. New York: John Wiley & Son, Inc.

Bradley, L. and Stewart, K. (2003). The diffusion of online banking. *Journal of Marketing Management 19(10),* 1087 -1109

Brancik, K. C. (2007). *Insider computer fraud.* New York: CRC Press.

Brannen, J. (1994). 'Combining qualitative and quantitative approaches: an overview' in J. Brannen (ed) *Mixing methods: qualitative and quantitative research.* Ashgate Publishing Limited, England Pgs. 3-37

Brase, C. H., & Brase, C. P. (2007). *Understandable statistics: Concepts and methods.* London: Cengage.

Breuer, J. B. (2006). Problem bank loans, conflicts of interest, and institutions. *Journal of Financial Institutions, 2,* 266-285.

British Broadcasting Corporation (BBC) (2006). Kenya's Goldenberg Affair, March 15, 2006). Available at: http://news.bbc.co.uk/1/hi/business/4808618.stm [Accessed on 2 February 2011]

Broadman, H. G., & Isik, G. (2007). *Africa's silk road: China and India's new economic frontier.* Washington, DC: World Bank.

Brody, R. (2010). Beyond the basic background check: hiring the 'right' employees. *Management Research Review, 33 (3),* 210-223

Brownridge, M. (1998). *Banking in Africa: the impact of financial sector reform since independence*. Oxford: James Currey Ltd/Africa World Press Inc

Brownridge, M. (1998b). *The causes of financial distress in local banks in Africa and Implications for Prudential Policy*. UNCTAD OSG/DP/132. Geneva, Switzerland

Bryman, A. (1988). *Quantity and Quality in Social Research*. London: Unwin Hyman.

Bryman, A. (1989). *Research Methods and Organisation Studies*. London: Unwin Hyman

Bryman, A. (1994). 'Quantitative and qualitative research: further reflections on their integration' in J. Brannen (ed) *Mixing methods: qualitative and quantitative research.* Ashgate Publishing Limited, England Pgs. 57-78

Bryman, A. (2004) Social Research Methods. Second edition. Oxford: Oxford University Press.

Buckley, A. (2004). *Multinational Finance*. London: Pearson Education Limited.

Burgess, A and Akers, R. L (1966). A Differential Association- Reinforcement Theory of Criminal Behaviour. *Social Forces, 1*: 128-147

Busch, A. (2009). *Banking regulation and globalization.* Oxford: Oxford University Press.

Button, M., Johnston, L., Frimpong, K., & Smith, G. (2007). New directions in policing fraud: The emergence of the counter fraud specialist in the United Kingdom. *International Journal of the Sociology of Law, 35*, 192-208.

Candy, P. (1991). *Self direction for life long learning*. San Francisco: Jossey-Bass

Canhoto, A. I., & Backhouse, J. (2007). Profiling under conditions of ambiguity - an application in the financial services industry. *Journal of Retailing and Consumer Services, 14*, 408-419.

Canter, D. (2004). Offender profiling and investigative psychology. *Journal of Investigative Psychology and Offender Profiling*, *1* (1), 1-15.

Capital Markets Authority, Kenya (2011). Available at: http://www.cma.or.ke/index.php?option=com_content&task=view&id=4&Itemid=31 [Accessed on 1 March 2011]

Caprio, G. Jnr. (1997). Safe and sound banking in developing countries: We're not in Kansas anymore. *Policy Research Working paper* No.1739. Washington, DC: World Bank

Carey, J.T. (1978). *Introduction to Criminology*. Englewood Cliffs, New Jersey: Prentice-Hall

Central Bank of Kenya. (2011). *Central Bank of Kenya Main Page*. Available at: http://www.centralbank.go.ke/ [Accessed on 4 April 2011]

Central Bank of Kenya (2010). Mergers and Acquisitions. Available at: http://www.centralbank.go.ke/financialsystem/banks/mergers.aspx [Accessed on 20 September 2010]

Central Bank of Kenya (2010b). Conversions. Available at: http://www.centralbank.go.ke/financialsystem/banks/conversions.aspx Retrieved on 20/9/10 [Accessed on 20 September 2010]

Central Bank of Kenya. (2010c, December). *Monthly Economic Review*. Available at: http://www.centralbank.go.ke/publications/Default.aspx [Accessed on 2 April 2011]

Central Bank of Kenya. (2008). Banking crises, failures and closures in post-independence Kenya. Available at: http://www.centralbank.go.ke/dpfb/background.aspx [Accessed on 21 January 2011]

Central Bank of Kenya. (2008b). Central bank of Kenya. Available at: http://www.centralbank.go.ke/financialsystem/banks/Introduction.aspx [Accessed on 20 September 2010]

Central Bank of Kenya. (2008c). Background information. Available at: http://www.centralbank.go.ke/about/default.aspx [Accessed on 21 January 2011]

Central Bank of Kenya. (2007). Commercial Banks and Mortgage Financial institutions Available at: http://www.centralbank.go.ke/financialsystem/banks/Introduction.aspx Retrieved on 20/6/10 [Accessed on 20 June 2010]

Central Bank of Kenya. (2003, September). *Payment System in Kenya*. Available at: http://www.google.com/url?sa=t&source=web&cd=2&sqi=2&ved=0CBcQFjAB&url=http%3A%2F%2Fwww.centralbank.go.ke%2Fdownloads%2Fnps%2Fnps%2520old%2Fpsk.pdf&rct=j&q=kenya%20bankers%20association&ei=TIucTPVCwf-WB7ie8JAK&usg=AFQjCNEqIXDdqT727_o8w5zPGO49H6Q0JA [Accessed on 16 September 2010]

Centre for Corporate Governance (2004). A study of Corporate Governance Practices in the Commercial Banking Sector in Kenya

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. International Journal of Accounting Information Systems , 12 (2), 152-160.

Chartered Institute of Management Accountants (2008). Fraud Risk Management: A guide to good practices. Available at: http://www1.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf [Accessed on 30 April 2012]

Chhaochharia, V., & Laeven, L. (2009). Corporate governance norms and practices. *Journal of Financial Intermediation, 18*, 405-431.

Claessens, S. & Horen, N.V. (2008). Location Decisions of Foreign Banks and Institutional Competitive Advantage. Available at: http://www.wto.org/english/res_e/reser_e/gtdw_e/wkshop08_e/claessens_e.pdf . [Accessed on 14/7/11]

Claessens, S., Jansen, M. (2000). The Internationalization of Financial Services: Issues and Lessons for Developing Countries. Dordrecht, Holland: Kluwer.

Cloninger, D. O., & Waller, E. R. (2000). Corporate fraud, systematic risk, and shareholder enrichment. *Journal of Socio-Economics, 29*, 189-201.

Cloward, R. A., & Ohlin, L. E. (1966). *Delinquency and opportunity.* New York: Free Press.

Consultative Group to Assist the Poor (2011). Regulating Banking Agents. World Bank, CGPA No.68, March 2011. Available at: http://www.cgap.org/gm/document-1.9.50419/FN68.pdf [Accessed on 2 July 2011]

Cook, T.D. & Reichardt, C.S. (1979). *Qualitative and Quantitative Methods in Evaluation Research.* London: Sage Publications.

Coram, P., Ferguson, C., & Moroney, R. (2008). Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud. Accounting and Finance, 48 (4), 543-559.

Costello, B. (1997). On the logical adequacy of cultural transmission theories. *Theoretical Criminology, 1* (4), 403-428.

Cressey, D. (1973). *Other People's Money: A study in the social psychology of embezzlement*. New Jersey: Patterson Smith Publishing Corporation

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). London: Sage Publications.

Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research.* London: Sage Publications.

Crocker, K. J., & Morgan, J. (1998). Is honesty the best policy? Curtailing insurance fraud through optimal incentive contracts. *The Journal of Political Economy, 106* (2), 355-375.

Crotty, M. (1998). *The Foundations of Social Research: Meaning and perspective in the research process*. London: Sage Publications

Crutchley, C. E., Jensen, M., & Marshall, B. B. (2007). Climate for Scandal: Corporate Environments that Contribute to Accounting Fraud. *Financial Review, 42* (1), 53-73.

Çule, M., & Fulton, M. (2009). Business culture and tax evasion: Why corruption and the unofficial economy can persist. *Journal of Economic Behaviour and Organisation, 73 (3),* 811-822.

Dahan, N. M., Doh, J. P., Oetzel, J., & Yaziji, M. (2010). Corporate-NGO Collaboration: Co-creating New Business Models for Developing Markets. *Long Range Planning, 43 (2-3),* 326-342.

Daly, K. (1989). Gender and varieties of white-collar crime. *Criminology, 27:* 769-793.

Davia, H. R., Coggins, P. C., & Wideman, J. C. (2000). *Accountant's guide to fraud detection and control.* London: John Wiley and Sons.

Day, R. (2010). *Applying the Fraud Triangle Model to the Global Credit Crisis*. Retrieved from Nordicum-Mediterraneum (Icelandic E-Journal of Nordic and Mediterranean Studies) 5(1). Available at: http://nome.unak.is/nm/5-1/12-reflection-on-the-economic-crisis-/236-applying-the-fraud-triangle-model-to-the-global-credit-crisis [Accessed on July 1, 2011]

De Haas, R., & Van Lelyveld, I. (2010). Internal capital markets and lending by multinational bank subsidiaries. *Journal of Financial Intermediation, 19*, 1-25.

De Maria, W. (2009). Business, ethnography and the global economic crisis: Paradigm power in the African "corruption" debate. *Critical Perspectives on International Business, 5 (4),* 263-284.

Debreceny, R., Lee, S., Neo, W., & Toh, J. (2005). Employing generalized audit software in the financial services sector: Challenges and opportunities. *Managerial Accounting Journal, 20 (6),* 605-618.

Demirgüç-Kunt, A., & Detragiache, E. (1998). The determinants of banking crises in developing and developed countries. *International Monetary Fund Staff Papers, 45 (1),* 81-109.

Demirguc-Kunt, A., & Detragiache, E. (2002). Does deposit insurance increase banking system stability? An empirical investigation. *Journal of Monetary Economics, 49*, 1373-1406.

Denzin, N. and Lincoln, Y. (1994). *Introduction: entering the field of the qualitative research*. In N. Denzin and Y. Lincoln (eds.), *Handbook of Qualitative Research.* London: Sage Publications.

Denzin, N. K. & Lincoln, Y.S (2003). *Strategies of qualitative inquiry*. London: Sage Publications.

Dixon, R., Ritchie, J., & Siwale, J. (2007). Loan officers and loan 'delinquency' in microfinance: A Zambian case. *Accounting Forum, 31*, 47-71.

Doidge, C., Karolyi, G. A., & Stulz, R. M. (2007). Why do countries matter so much for corporate governance? *Journal of Financial Economics, 86*, 1-39.

Dorminey, J.W., Fleming A.S., Kranacher, M., Riley, R.A. (2010). Beyond the fraud triangle: enhancing the deterrence of economic crimes. *The CPA Journal, July,* 17-23.

Domfeh, K. A., & Bawole, J. N. (2011). Muting the whistle-blower through retaliation in selected African countries. *Journal of Public Affairs*, (In press).

Doyle,J., Ge, W., McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. *Journal of Accounting and Economics, 44*:193–223

Dozier, J.B. and Miceli, M.P. (1985). Potential Predictors of whistle-blowing: A Prosocial Behaviour Perspective. *Academy of management Review, 10*, 823-836.

Drew, S. A., Kelley, P. C., & Kendrick, T. (2006). CLASS: Five elements of corporate governance to manage strategic risk. *Business Horizons, 49*, 127-138.

Dunn, P. (2004). The Impact of Insider Power on Fraudulent Financial Reporting. *Journal of Management, 30* (3), 397-412.

Durkheim, E. (1964). *The Division of labour of society*. New York: Free Press.

Durtschi, C., Hillison, W., & Pacini, C. (2004). The effective use of Benford's Law to assist in detecting fraud in accounting data. *Journal of Forensic Accounting, 1524-5586/Vol.V*, 17-34.

Dworkin, T.M. & Baucus, M.S. (1998). Internal vs External Whistleblowers: A Comparison of Whistleblowing processes. *Journal of Business Ethics, 17,* 1281-1298.

Edge, M. E., & Sampaio, P. R. (2009). A survey of signature based methods for financial fraud detection. *Computers & Security, 28,* 381-394.

Elliot, R. K., & Willingham, J. J. (1980). *Management fraud: Detection and deterrence.* New York: Petrocelli Books.

Emory, W., and Copper, D. (1991). *Business Research Methods*, 4th ed. USA: Irwin Inc

Evanoff, D., & Kaufmann, G. (2005). *Systemic financial crises: Resolving large bank insolvencies* . London: World Scientific.

Evans, J., & Dadzie, K. (1998). Corporate governance and the fragility of banking systems in developing countries: An analysis of a credit market in Ghana. *Global Finance Journal, 9 (1),* 109-125.

Family News Forum. (2010). The Kenya Goldenberg Scandal, December 3, 2010. Available at: http://www.news-kenya.com/2010/12/the-kenya-goldernberg-scandal/ [Accessed on 1 April 2011]

Feldman, R. (2001). An economic explanation for fraud and abuse in public medical care programs. *Journal of Legal Studies, 30,* 569

Felson, M., & Clarke, R. (1998). Opportunity makes the thief: Practical theory for crime prevention. *Police Research Series,* Paper 98.

Fernandez, A. I., & Gonzales, F. (2005). How accounting and auditing systems can counteract risk-shifting of safety-nets in banking: Some international evidence. *Journal of Financial Stability, 1 (3),* 465-500.

Fetterman, D. (1988). *Qualitative Approaches to Evaluation in Education: The Silent Scientific Revolution*. New York: Prager

Finch, E. (2010). Strategies of adaptation and diversification: The impact of chip and PIN technology on the activities of fraudsters. *Security Journal*, 7th June 2010.

Fisher, J., Harshman, E., Gillespie, W., Ordower, H., Ware, L., & Yeager, F. (2001). Privatising regulation: Whistleblowing and bounty hunting in the financial services industries. *Journal of Financial Crime, 8 (4),* 305-318.

Fisman, R., & Svensson, J. (2007). Are corruption and taxation really harmful to growth? Firm level evidence. *Journal of Development Economics, 83 (1),* 63-75.

Fleetwood, S. (1999). *Critical realism in economics: Development and debate.* London: Routledge.

Flick, U. (1998). *An introduction to qualitative research*. London: Sage Publications.

Fraud Act, 2006. Sections 1-4, UK Laws.

Free, C., & Macintosh, N. (2007). Management controls: The organizational fraud triangle of leadership, culture and control at Enron. Ivey Business Journal , 71 (6), 1-9.

Frimpong, G. (2007). Trends in ICT usage in small and medium scale enterprises in Ghana. *ATDF Journal, 4 (1),* 3-10.

Friedberg, E. (1993). Le Pouvoir et la Re`gle. Paris: Seuil

Friedrichs, D.O. (2004). Trusted Criminals, 2nd Ed. Belmont, CA: ITP/Wadsworth Publishing.

Frynas, J. G., & Paulo, M. (2006). A new scramble for African oil? Historical, political and business perspectives. *African Affairs*, *106*, 229-251.

Furst, K., Lang, W., & Nolle, D. (2002). Internet banking. *Journal of Financial Services Research*, *22*, 95–117.

Garrick, John. (1999). Doubting the philosophical assumptions of interpretive research. *International Journal of Qualitative Research in Education 12 (2),* 147-156.

Gavious, I. (2007). Alternative perspectives to deal with auditors' agency problem. *Critical Perspectives on Accounting, 18,* 451-467.

Gaylord, M.S. and Galliher, J.F. (1988). The Criminology of Edwin Sutherland. New Brunswick, NJ: Transaction Books.

Ghosh, M. (2010). Telecoms fraud. *Computer Fraud and Security*, *7*, 14-17.

Giannetti, C., Jentzsch, N. & Spagnolo, G. (2010). Information-Sharing and Cross-Border Entry in European Banking. *ECRI Research Report No. 11,* February 2010, Belgium.

Gikandi, J.W. and Bloor, C. (2010). Adoption and effectiveness of electronic banking in Kenya. *Electronic Commerce Research Applications 9,* 277-282.

Glaser, D. (1956). Criminality Theories and Behavioural Images. *American Journal of Sociology 61 (5),* 433-444.

Goode, S., & Lacey, D. (2011). Detecting complex account fraud in the enterprise: The role of technical and non-technical controls . *Decision Support Systems, 50 (4),* 702-714.

Goodwill, A. M., Alison, L. J., & Beech, A. R. (2009). What works in offender profiling? A comparison of typological, thematic, and multivariate models. *Behavioural Science and the Law*, *27* (4), 507-529.

Graham, J. R., Li, S., & Qiu, J. (2008). Corporate misreporting and bank loan contracting. *Journal of Financial Economics, 89*, 44-61.

Green, B. P., & Reinstein, A. (2004). Banking industry financial statement fraud and the effects of regulation enforcement and increased public scrutiny. *Research in Accounting Regulation, 17*, 87-106

Greenbaum, S. I., & Thakor, A. V. (2007). *Contemporary financial intermediation* (2nd ed.). London: Elsevier Academic Press.

Greenlee, J., Fischer, M., Gordon, T., & Keating, E. (2007). An investigation of fraud in non-profit organisations: Occurrences and deterrents. *Non-profit and Voluntary Sector Quarterly, 36 (4),* 676-694.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*, 597-607.

Government of Kenya (2008). Government of Kenya Act of Parliament. Kenya Communication (Amendments) Bill, Kenya.

Grix, J. (2004). *The foundations of research.* London: Macmillan.

Grundberg, I. (1998). Double Jeopardy: Globalization, liberalization and the fiscal squeeze. *World Development, 26 (4),* 591-605

Guba, E.G. & Lincoln, Y.S. (1994) Competing Paradigms in Qualitative Research. Chapter 6 in Denzin, N.K. and Lincoln, Y.S. (Eds) *Handbook of Qualitative Research.* London: Sage Publications.

Guba, E.G. (1990). *The paradigm dialogue.* London: Sage Publications.

Hamlyn, D. W. (1995). Epistemology, History of. Oxford: Oxford University Press.

Haniffa, R., & Hudaib, M. (2007). Locating audit expectations gap within a cultural context: The case of Saudi Arabia. *Journal of International Accounting, Auditing and Taxation, 16,* 179-206.

Hartmann-Wendels, T., Mählmann, T., & Versen, T. (2009). Determinants of banks' risk exposure to new account fraud - Evidence from Germany. *Journal of Banking and Finance, 33*, 347-357.

Haugen, S., & Selin, J. R. (1999). Identifying and controlling computer crime and employee fraud. *Industrial Management & Data Systems, 99 (8),* 340-344.

Healy, M., & Perry, C. (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative Market Research: An International Journal, 3*, 118-126.

Heimer, K. (2000). Changes in the gender gap in crime and women's economic marginalization. In G. LaFree (Ed.), *Criminal Justice 2000: The nature of crime, continuity and change, 1*, 1-57. Washington DC: National Institute of Justice.

Henn, M., Weinstein, M., & Foard, N. (2009) *A Short Introduction to Social Research*. London: Sage Publications.

Heugens, P., & Otten, J. (2007). Beyond the dichotomous worlds' hypothesis: Toward a plurality of corporate governance logics. *Corporate Governance: An International Review, 15* (6), 1288-1300.

Hillison, W., Pacini, C., & Sinason, D. (1999). The internal auditor as fraud-buster. *Managerial Accounting Journal, 14 (7),* 351-363.

Hoffman, D. G. (2002). *Managing operational risk: 20 firmwide best practice strategies.* London: John Wiley and Sons.

Hofstede, G., & Hofstede, G. J. (2005). *Cultures and organisations: Software of the mind.* London: McGraw-Hill.

Hofstede, G. (1980). *Culture's Consequences: International Differences in Work Related Values*. Beverly Hills, CA: Sage Publications

Hollinger, R. C., & Clark, J. P. (1983). Deterrence in the workplace: Perceived certainty, perceived severity and employee theft. *Social Forces, 62,* 398-418.

Holmes, S.A., Strawser, J.W. & Welch, S.T. (2000). Fraud in the Governmental and private sectors. *Journal of Public Budgeting, Accounting and Financial Management, 12(3),* 345, 25pgs

Holtfreter, K. (2005). Is occupational fraud "typical" white-collar crime? A comparison of individual and organisational characteristics. *Journal of Criminal Justice, 33,* 353–365.

Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Support Systems, 46* (4), 853-864.

Homazi, A. N., & Giles, S. (2004). Data mining: A competitive weapon for banking and retail industries. *Information Systems Management, 21 (2),* 62-71.

Horrocks, M., Ramaswamy, V., & Rupp, K. (2008). Financial reforms in Chinese banking: The impact on personal lending and operational efficiency. *Business Horizons, 51*, 511-517.

Hoshmand, L.T. (2003). Can lessons of history and logical analysis ensure progress in psychological science? *Theory and Psychology*, *13*: 39–44.

Humphrey, C., & Turley, S. (1993). Protecting against detection: The case of auditors and fraud? *Accounting, Auditing & Accountability Journal, 6*, 39-62.

Ikiara, G.K., Nyandemo, S.M. & Ikiara, M.M. (2003). *Kenya's Service Sector: Emerging National, Regional and Global Issues.* African Economic Research Consortium (AERC) Collaborative Research Project on African Imperatives in the New World Order: Draft Paper August 2003.

Irungu, G. (2011). *Fraudsters find holes in new bank system*. Business Daily, May 4, 2011. Available at: http://www.businessdailyafrica.com/Fraudsters+find+holes+in+new+bank+system/-/539552/1155704/-/jvuuifz/-/index.html [Accessed on 2nd July 2011]

Jaffe, J. F. (1974). The effects of regulation changes on insider trading. *The Bell Journal of Economics and Management Science, 5* (1), 93-121.

James, C. (1991). The losses realized in bank failures. *The Journal of Finance, 46 (4),* 1223-1242.

James, K. L. (2003). The effects of internal audit structure on perceived financial statement fraud prevention. *Accounting Horizons, 17 (4),* 315-327.

Jayawardhana, W. (2009). LTTE is involved in credit card fraud in Kenya says paper. *Ministry of Defence, Democratic Socialist Republic of Sri Lanka.* Available at: http://www.defence.lk/new.asp?fname=20080725_04 [Accessed on 11 October 2010]

Johnson, R. A., & Bhattacharyya, G. K. (2009). *Statistics: Principles and Methods.* London: John Wiley and Sons.

Johnson, R.B., and Onwuegbuzie, A.J., (2004). Mixed Methods Research: A Research paradigm whose time has come. *Educational Researcher, Vol.33, No.7: 14-26.*

Kaler, J. (2003). Differentiating stakeholder theories. *Journal of Business Ethics, 46* (1), 71-83.

Kamoche, K. (2011). Contemporary developments in the management of human resources in Africa . *Journal of World Business, 46 (1),* 1-4.

Kane, E. J., & Rice, T. (2001). Bank runs and banking policies; Lessons for African policy makers. *Journal of African Economics, 10,* 36-71.

Kaptein, M. (2008). Developing and Testing a Measure for the Ethical Culture of Organisations: The Corporate Ethical Virtues Model. *Journal of Organisational Behaviour, 29,* 923-947.

Keenan, J. P. (2000). Blowing the whistle on less serious forms of fraud: A study of executives and managers. Employee Responsibilities and Rights Journal , 12 (4), 199-217.

Kenya Anti-Corruption Commission. (2010). *About KACC: Vision & Mission*. Available at: http://www.kacc.go.ke/default.asp?pageid=3 [Accessed on 17 September 2010]

Kenya Commercial Bank. (2011). Historical Background. Available at: http://www.kcbbankgroup.com/ke/index.php?option=com_content&task=view&id=44&Itemid=314 [Accessed on 14 February 2011]

Kenya Credit Information Sharing Initiative. (2010). *Kenya Credit Information Sharing Initiative: What is Credit Information Sharing (CIS)?* Available at: http://www.kenyacreditinfo.com/ [Accessed on 27 September 2010]

Kenya Digital Study (2010). Kenya ICT and TNS Research International. Available at: http://www.ictworks.org/network/ictworks-network/31 [Accessed on 14 October 2010]

Kerlinger, F.N. (1973). *Foundations of Behavioural Research*. USA: Holt, Rinehart and Winston.

Kim, D. J., Steinfield, C., & Lai, Y. (2008). Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems, 44 (4),* 1000-1015.

KIPPRA (2005). Financial Sector in the economic recovery process: Role, Challenges and Future. Kenya Institute for Public Policy Research and Analysis.

KPMG (2005). African Fraud and Misconduct Survey. Available at http://www.kpmg.co.za/images/naledi/pdf%20documents/mc261%20fraud%20survey%2005.pdf [Accessed on 29 April 2007]

KPMG (2007). Profile of a Fraudster Survey 2007. KPMG Forensic, Switzerland. Available at: http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf [Accessed on 28 January 2011]

KPMG (2008). Fraud Trends: The KPMG Fraud Barometer.

Krambia-Kapardis, M, & Kapardis, A. (2004). Enhancing fraud prevention and detection by profiling fraud offenders. *Criminal Behaviour and Mental Health 14*: 189-201.

Krambia-Kapardis, M. (2002). Fraud Victimization Study: Cyprus experience, Nicosia: Ernst and Young, Cyprus.

Krambia-Kapardis, M. (2001) Fraud detection model: A must for auditors. *Journal of Financial Regulation and Compliance 10(3):* 266-278.

Kranacher, M.J., Riley, R.A. and Wells, J.T. (2011). Forensic Accounting and Fraud Examination. London: John Wiley and Sons.

Krugman, P., & Wells, R. (2006). *Economics.* New York: Worth Publishers.

KTN. (2010). *Banking fraud report shocker*. Retrieved from Kenya Television Network (KTN) Business Today: http://www.youtube.com/watch?v=Ao-A9dB44IM

Kuhn, J. R., & Sutton, S. G. (2006). Learning from Worldcom: Implications for fraud detection through continuous assurance. Journal of Emerging Technologies in Accounting , 3, 61-80

Labovitz, G. (2005). Well aligned: Using alignment to achieve extraordinary results. Builders and leaders, Boston University School of Management (pp. 24– 25).

Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of Financial Economics, 93*, 259-275.

Lanza, R. B., Gilbert, S., & Lamoreaux, M. (2007). A risk-based approach to journal entry testing. *Journal of Accountancy, 20 (1),* 32-35

Laub, J.H., (2006). Edwin H. Sutherland and the Michael-Adler Report: Searching for the Soul of Criminology Seventy years later. *Criminology, 44(2),* 235-464

Ledgerwood, J. & White, V. (2006) *Transforming microfinance institutions: providing full financial services to the poor*. Washington: International Bank for Reconstruction and Development/World Bank Available at: http://books.google.co.uk/books?id=_VEW4t6ZuroC&pg=PA383&lpg=PA383&dq=job+rotation+and+fraud&source=bl&ots=BtnslhSzlL&sig=OltJwE8rXoU7v-wPEE20sIdHd0c&hl=en#v=onepage&q=job%20rotation%20and%20fraud&f=false [Accessed on 3 March 2011]

Lee, M. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications, 8 (3),* 130-141.

Lee, S. H., & Hong, S. J. (2010). Corruption and subsidiary profitability: US MNC subsidiaries in the Asia Pacific region . Asia Pacific Journal of Management .

Lee, T. A., Clarke, F., & Dean, G. (2008). The dominant senior manager and the reasonably careful, skilful, and cautious auditor. *Critical Perspectives on Accounting, 19*, 677-711.

Licht, A. N., Goldschmidt, C., & Schwartz, S. H. (2005). Culture, law and corporate governance. *International Review of Law and Economics, 25*, 229-255.

Lin, Y. (2005). Corporate Governance, Leadership Structure and CEO Compensation: evidence from Taiwan. *An International Review Journal 13 (6)*: 824.

Lin, Z. J. (2004). Auditor's responsibility and independence: Evidence from China. *Research in Accounting Regulation, 17*, 167-190.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. London: Sage Publications.

Macey, J., & O'Hara, M. (2003). The corporate governance of banks. *Federal Reserve Bank New York (FRBNY) Economic Policy Review*, 91-107.

Macey, J.R, and O'Hara, M. (2001). The Corporate Governance of Banks. *Federal Reserve Bank of New York (FRBNY) Economic Policy Review*. Financial Stability Forum.

Macquarrie, J. (1973). *The Concept of Peace*. London: S.C.M. Press

Mannan, M., & Van Oorschot, P. C. (2009). Reducing threats from flawed security APIs: The banking PIN case. *Computers & Security, 28*, 410-420.

Matsueda, R. L. (1988). The Current State of Differential Association Theory. *Crime and Delinquency, 34(3),* 277-306.

Mawhinney, T. C. (2009). Identifying and extinguishing dysfunctional and deadly organisational practices. *Journal of Organisational Behaviour Management, 29 (3/4),* 231-256.

May, C. (2003). Dynamic corporate culture lies at the heart of effective security strategy. *Computer Fraud and Security, 5*, 10-13.

Mayes, D. G. (2005). Who pays for bank insolvency in transition and emerging economies? *Journal of Banking and Finance, 29*, 161-181.

Maynard, M. (1994). Methods, practice and epistemology: The debate about feminism and research. London: Taylor & Francis.

Mbaku, J. M. (2007). *Corruption in Africa: Causes, consequences and clean-ups.* London: Lexington Books.

McBarnet, D. (2003). When compliance is not the solution but the problem: From changes in law to changes in attitude. In V. A. Brathwaite (Ed.), *Taxing democracy: understanding tax avoidance and evasion* (pp. 229-245). London: Ashgate.

McDaniel, C. & Gates, R. (2007) *Marketing Research.* 7th ed. London: John Wiley & Sons.

McGee, R. W. (2008). An overview of corporate governance practices in South Africa. In *Corporate Governance in Developing Economies: Country Studies of Africa, Asia and Latin America* (pp. 287-291). London: Springer.

Merton, R.K. (1938). Social Structure and Anomie. *American Sociological Review,* October, 672-82.

Merton, R.K. (1957). Social Theory and Social Structure. *Michigan Law Review, Chp.66, Sect.1529*, 131-160.

Meyer, M., Roodt, G., & Robbins, M. (2011). Human resources risk management: Governing people risks for improved performance. *South African Journal of Human Resources Management , 9* (1).

Mezirow, J. (1996). Contemporary paradigms of learning. *Adult Education Quarterly, 46(3)*: 158-173.

Miceli, M.P. and Near, J.P. (1985). Characteristics of Organisational Climate and Perceived Wrongdoing Associated with Whistleblowing Decisions. *Personnel Psychology 38,* 525-544.

Miceli, M.P., Near, J.P and Dworkin, T.M. (2008b). *Whistleblowing in Organizations.* New York: Routledge.

Michel, M. (2008). Financial crimes: the constant challenge of seeking effective prevention solutions. *Journal of Financial Crime, 15 (4),* 383-397.

Miles, M.B. & Huberman, A.M. (1994). *Qualitative Data Analysis: an expanded Sourcebook.* London: Sage Publications.

Milgrom, P. R., North, D. C., & Weingast, B. R. (1990). The role of institutions in the revival of trade: The law merchant, private judges and the Champagne fairs. *Economics and Politics, 2* (1), 1-21.

Mintzberg, H. (1983). An Emerging Strategy of Direct Research in Van Maanen, J. (Ed) *Qualitative Methodology.* London: Sage Publications.

Mishkin, F. S. (1999). Financial consolidation: Dangers and opportunities. *Journal of Banking and Finance, 23 (2-4),* 675-692.

Mishkin, F. S. (2006). *The economics of money, banking, and financial markets* (8th ed.). London: Pearson Addison Wesley.

Mitchell, A., & Sikka, P. (1996). Sweeping it under the carpet: The role of accountancy firms in money laundering. *Critical Perspectives on Accounting Symposium,* (p. 37).

Moeller, R. R. (2004). *Sarbanes-Oxley and the new accounting rules.* London: John Wiley and Sons.

Mohan, G., Brown, E., Milward, B., & Zack-Williams, A. B. (2000). *Structural adjustment: Theory, practice and impacts.* New York: Psychology Press.

Moore, D. S., & Notz, W. I. (2006). *Statistics: Concepts and controversies.* London: MacMillan.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives, 23 (3),* 3-20.

Moorthy, M. K., Seetharaman, A., Somasundaram, N. R., & Gopalan, M. (2009). Preventing employee theft and fraud. *European Journal of Social Sciences, 12 (2),* 259-268.

Moyo, D., & Ferguson, N. (2010). *Dead Aid: Why Aid Is Not Working and How There Is a Better Way for Africa.* London: Macmillan.

Muhoro, J., & McGee, R. (2008). Corporate governance and the timeliness of financial reporting: A comparative study of Kenya and the United States of America. In *Corporate Governance in Developing Economies: Country Studies of Africa, Asia and Latin America* (pp. 113-118). London: Springer.

Mullins, L.J. (1999). *Management and Organizational Behaviour*. 5th Edition. London: Pitman Publishing.

Murdoch, S. J., Drimer, S., Anderson, R., & Bond, M. (2010). Chip and pin is broken. *2010 IEEE Symposium on Security and Privacy* (pp. 433-446). New York: IEEE.

Murphy, D. S., & Robinson, M. B. (2008). The maximizer: Clarifying Merton's theories of anomie and strain. *Theoretical Criminology, 12* (4), 501-521.

Murphy, K. (1993). Honesty in the Workplace. Pacific Grove, CA: Brooks/Cole Publishing.

Murray, B.C., Kelly, J.S., Ganzi, J.T. (1997) *Review of Environmental Risk Management at Banking Institutions and Potential Relevance of ISO 14000*, Working Paper RTI Project Number 5774-4, Research Triangle Institute.

Mustaine, E. E., & Tewksbury, R. (2002). Workplace theft: An analysis of student-employee offenders and job attributes. *American Journal of Criminal Justice, 27* (1), 111-127.

Mwanza, K. (2010). Lenders to begin sharing clients' history with CRBs. *Business Daily* [online], 14 July 2010. Available at: http://www.businessdailyafrica.com/Company%20Industry/Lenders%20to%20begin%20sharing%20clients%20history%20with%20CRBs/-/539550/957446/-/view/printVersion/-/r6dwv4z/-/index.html [Accessed on 29 February 2011]

Mwega, F. (n.d). Chapter 10 - Financial Sector Reforms in Eastern and Southern Africa. Available at: http://www.idrc.ca/en/ev-56345-201-1-DO_TOPIC.html [Accessed on 12 February 2011]

Ndungu, N. and Etemesi, R. (2010). Kenya: How Local Banks are Coping with Fraud. *Daily Nation* [online] 9 August 2010. Available at: http://allafrica.com/stories/201008091253.html [Accessed on 27 September 2010]

Nier, E., & Baumann, U. (2006). Market discipline, disclosure and moral hazard in banking. *Journal of Financial Intermediation, 15* (3), 332-361.

Netemeyer, R.G., Bearden, W.O. & Sharma, S. (2003). *Scaling Procedures: Issues and Applications*. London: Sage Publications.

Newenham-Kawindi, A. (2011). Human resource strategies for managing back-office employees in subsidiary operations: The case of two investment multinational banks in Tanzania. *Journal of World Business, 46* (1), 13-21.

Neu, D., Rahaman, A. S., Everett, J., & Akindayomi, A. (2010). The sign value of accounting: IMF structural adjustment programs and African banking reform . *Critical Perspectives on Accounting, 21 (5)*, 402-419.

Ngugi, R.W. and Kabubo, J.W (1998). Financial Sector Reforms and Interest Rate Liberalization: The Kenyan Experience. African Economic Research Consortium, Research Paper 72.

Nord, G. D., Nord, J. H., & Zu, H. (2005). An investigation of the impact of organization size on data quality issues. Journal of Database Management , 16 (3), 58-71.

Norusis, M. J. (2008). *SPSS Statistics 17.0 guide to data analysis.* London: Prentice Hall.

Nunez, J. (2007). Can self regulation work?: a story of corruption, impunity and cover-up. *Journal of Regulatory Economics*, *31*, 209-233.

Okwembah, D. (2010). Kenya: Alarm as bank employees siphon out Sh2.4bn through "inside jobs". *Daily Nation* [online], 10 July. Available at: http://allafrica.com/stories/201007120388.html [Accessed on 27 September 2010]

OECD. (2002). Foreign direct investment for development: maximising benefits, minimising costs. London: OECD Publishing.

Ombati, C. (2010) Banks lost Sh761 million to fraud, says report. *The Standard Newspaper* [online], 29 September 2010.
Available at: http://www.standardmedia.co.ke/InsidePage.php?id=2000018760&cid=4 [Accessed on 29 September 2010]

Oman, C.P. (2001). Corporate Governance and National Development. OECD. Development Centre Technical Papers, Number 180.

Omar, N. B., & Mohamad Din, H. F. (2010). Fraud diamond risk indicator: An assessment of its importance and usage. *International Conference on Science and Social Research* (pp. 607-612). Kuala Lampur, Malaysia: IEEE.

Omurgonulsen, M., & Omurgonulsen, U. (2009). Critical thinking about creative accounting in the face of a recent scandal in the Turkish banking sector. *Critical Perspectives on Accounting*, *20*, 651-675.

Oremade, T. (1988): Auditng and Investigation. Lagos, West African Book Publishers

Oshikoya, T. W. (2010). Monetary and financial integration in West Africa. London: Taylor & Francis.

Owojori, A. A., Akintoye, I. R., & Adidu, F. A. (2011). The challenge of risk management in Nigerian banks in the post consolidation era. *Journal of Accounting and Taxation, 3* (2), 23-31.

Paliwal, M., & Kumar, U. A. (2009). Neural networks and statistical techniques: A review of applications. *Expert Systems with Applications, 36*, 2-17.

Palmer, I., Dunford, R., & Akin, G. (2008). *Managing organisational change.* London: McGraw-Hill.

Palmer, M. (2000). Records management and accountability versus corruption, fraud and maladministration. Records Management Journal, 10 (2), 61-72.

Pasiouros, F., Tanna, S., & Zopounidis, C. (2009). The impact of banking regulations on banks' cost and profit efficiency: Cross-country evidence. *International Review of Financial Analysis, 18,* 294-302.

Passas, N. (1990). Anomie and corporate deviance. *Crime, Law and Social Change, 14* (2), 157-178.

Passas, N. (1999). Continuities in the anomie tradition. In F. Adler, & W. Laufer (Eds.), *The legacy of anomie theory.* New York: Transaction Publishers.

Patterson, R. (2007). African brain circulation: Beyond the drain-gain debate. Leiden: BRILL.

Patton, M.Q. (1986). *Utilization-focused Evaluation*. London: Sage Publications.

Patton, M.Q. (1990). Qualitative Evaluation and Research Methods. 2nd edition. London: Sage Publications.

Payne, B. D., & Richards, W. K. (2008, May/June). A brief introduction to usable security. *IEEE Internet Computing*, 30-38.

Petrou, A. P. (2009). Foreign market entry strategies in retail banking: Choosing an entry mode in a landscape of constraints. *Long Range Planning, 42,* 614-632.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2005). A comprehensive survey of data mining-based fraud detection research. (*Artificial Intelligence Review).* Clayton School of Information Technology, Monash University.

Phua., C., Alahakoon, D., & Lee, V. (2004). Minority report in fraud detection: Classification of skewed data. *Sigkdd Explorations, 6 (1),* 50-59.

Pontell, H. N. (2005). Control fraud, gambling for resurrection, and moral hazard: Accounting for white-collar crime in the savings and loan crisis. *The Journal of Socio-Economics, 34*, 757-770.

Popoola, S.O. (2000). Scanning the Environment for Competitive Advantage: A Study of Corporate Banking Managers in Nigeria. *Libri, 50*, 210-216

Popper, K. (1959). The Logic of Scientific Discovery. Oxford: Oxford University Press.

Porter, D. (2003). Insider fraud: Spotting the wolf in sheep's clothing. *Computer Fraud & Security, 4,* 12-15.

Porter, B. (1997): *Auditors' responsibilities with respect to corporate fraud: a controversial issue*, in Sherer, M. and Turley, S. (Eds), 3rd ed., Current Issues in Auditing, Paul Chapman Publishing. London, Ch. 2:31-54.

Potter, E. J. (2002). Customer authentication: The evolution of signature verification in financial institutions. *Journal of Economic Crime Management, 1* (1).

PricewaterhouseCoopers. (2004). The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks. PricewaterhouseCoopers International Limited.

Prowse, S. (1997). The Corporate Governance System in Banking: What do we know? *BNL Quarterly Review*, March Issue.

Pryor, F. L. (2007). The economic impact of Islam on developing countries. *World Development, 35 (11),* 1815-1835.

Ramos, M. (2003). *Fraud detection in a GAAS Audit*. New York: American Institute of Certified Public Accountants (AICPA)

Razaee, Z. (2001). *Financial Institutions, valuations, mergers and acquisitions: the fair value approach*. London: John Wiley and Sons.

Razaee, Z. (2005). Causes, consequences, and deterrence of financial statement fraud . *Critical Perspectives on Accounting, 16* (3), 277-298.

Remenyi, D., Williams, B., Money, A. and Swartz, E. (1998). *Doing Research in Business and Management: An Introduction to Process and Method.* London: Sage Publications.

Republic of Kenya. (2005). Report of the Judicial Commission of Inquiry into the Goldenberg Affair

Riahi-Belkaoui, A. and Picur, R.D. (2000). Understanding fraud in the Accounting environment. *Managerial Finance (26)*: 11.

Risk Management Survey (2010). Central Bank of Kenya.

Robbins, P.S. and Coulter, M. (2012). *Management*. London: Pearson Education Limited.

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers and Security, 22* (4), 292-298.

Romero-Avila, D. (2007). Finance and growth in the EU: New evidence from the harmonisation of the banking industry. *Journal of Banking and Finance, 31*, 1937-1954.

Rose-Ackerman, S. (2002). "Grand" corruption and the ethics of global business. *Journal of Banking and Finance, 26*, 1889-1918.

Rousseau, G. J. (2005). Business ethics and corporate governance in Africa. *Business Society, 44* (1), 94-106.

Rusch, J. (2001). The Rising Trend of Internet fraud. *United States Attorneys' Bulletin*. Internet fraud Cybercrime II, *49 (3),* 6-12.

Saldana, J. (2009). The Coding Manual for Qualitative Researchers. London: Sage Publications Ltd.

Salehi, M., & Azary, Z. (2008). Fraud detection and audit expectation gap: Empirical evidence from Iranian bankers. *International Journal of Business and Management, 3* (10), 65-78.

Sankar, Y. (2003). Character not charisma is the critical measure of leadership excellence. *Journal of Leadership and Organisational Studies, 9 (4),* 45– 55.

Sardanis, A. (2007). *A venture in Africa: The challenges of African business.* London: IB Tauris.

Schein, E. H. (1996). Organisational culture and leadership. San Francisco: Jossey-Bass.

Schmidt, M. (2005). "Whistle blowing" regulation and accounting standards enforcement in Germany and Europe - an economic perspective. *International Review of Law and Economics, 25*, 143-168.

Schroth, P. W. (2005). The African Union Convention on Preventing and Combating Corruption. *Journal of African Law, 49,* 24-38.

Schutt, R. K. (2003). *Investigating the social world: The process and practice of research.* Newbury Park, CA: Pine Forge Press.

Seetharaman, A., Senthilvelmurugan, M. & Periyanayagam, R. (2004). Anatomy of computer accounting frauds. *Managerial Auditing Journal, 19 (8),* 1055-1072.

Shao, Y. P. (1999). Expert systems diffusion in British banking: Diffusion models and media factor. *Information & Management, 35*, 1-8.

Shen, C., & Chih, H. (2005). Investor protection, prospect theory, and earnings management: An international comparison of the banking industry. *Journal of Banking and Finance, 29*, 2675-2697.

Silverstone, H. & Davia, H. (2005). *Fraud 101: techniques and strategies for detection*. 2nd edition. London: John Wiley and Sons.

Silverstone, H. & Sheetz, M. (2004) *Forensic accounting and fraud investigation for non- experts*. London: John Wiley and Sons.

Silverstone, H., Sheetz, M., Pedneault, S., Rudewicz, F. (2012) *Forensic accounting and fraud investigation for non- experts*. New Jersey: John Wiley and Sons.

Simons, R. (1995). Control in an age of empowerment. *Harvard Business Review, 73(2),* 80– 88.

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

Singleton, T., Singleton, A., & Bologna, J. (2006). *Fraud auditing and forensic accounting.* London: John Wiley and Sons.

Skousen, C. J., & Wright, C. (2008). Contemporaneous risk factors and the prediction of financial statement fraud. *Journal of Forensic Accounting, IX*, 37-62.

Small, M. W. (2006). Management development: developing ethical corporate culture in three organisations. *Journal of Management Development, 25* (6), 588-600.

Smigel, E. O. (1956). Public attitudes toward stealing as related to the size of the victim organisation. *American Sociological Review, 21*, 3 – 20.

Smith, D., & Drudy, L. (2008). Corporate culture and organisational ethics. *Leadership and Business Ethics*, *25*, 165-176.

Smith, D. J. (2008). *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria.* Princeton, NJ: Princeton University Press.

Smith, H. J. (2003). The shareholders vs. stakeholders debate. *MIT Sloan Management Review*, *44* (4), 85-90.

Smith, R.G. (2003). Serious Fraud in Australia and New Zealand. Canberra: Australian Institute of Criminology.

Soral, H. B., Iscan, T. B., & Hebb, G. (2006). Fraud, banking crisis, and regulatory enforcement: Evidence from micro-level transactions data. *European Journal of Law and Economics, 21,* 179-197.

Steane, P., and Cockerell, R. (2005). Developing a Fraud Profile Method – A Step in Building Institutional Governance. Paper presented at Ethics and Integrity Conference: A Transatlantic Dialogue by the European Group of Public Administration.

Steffensmeier, D.J. (1993). National Trends in female arrest, 1960-1990: Assessments and recommendations for research. *Journal of Quantitative Criminology, 9,* 411- 441.

Stein, H. (1994). Theories of institutions and economic reform in Africa. *World Development, 22 (12),* 1833-1849.

Steward, A.M., Tittle, E. & Chappel, M. (2009). *Certified Information Systems Security Professional*. London: John Wiley and Sons.

Stiglitz, J.E., & Weiss, A. (1981). Credit rationing in markets with imperfect information, *American Economic Review*, *71*, 393-410.

Stremitzer, A. (2005). *Agency theory: Methodology, analysis.* London: Lang.

Stringer, C., & Carey, P. (2006). Internal control redesign: An exploratory study of Australian organisations. *Accounting, Accountability and Performance, 3 (1),* 1-20.

Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. *Electronic Commerce Research and Applications*, 247-263.

Summers, S. L., & Sweeney, J. T. (1998). Fraudulently misstated financial statements and insider trading: An empirical analysis. *The Accounting Review, 73* (1), 131-146.

Sutherland, E.H. (1949). *White Collar Crime*. New York: Dryden.

Sutherland, Edwin Hardin. (1974). Criminology (9th ed.). Philadelphia: Lippincott.

Sweeney, J., & Swait, J. (2008). The effects of brand credibility on customer loyalty. *Journal of Retailing and Consumer Services, 15 (3),* 179-193.

Szockyj, E., & Geis, G. (2002). Insider trading patterns and analysis. *Journal of Criminal Justice, 30,* 273-286.

Tadesse, S. (2006). The economic value of regulated disclosure: Evidence from the banking sector. *Journal of Accounting and Public Policy, 25,* 32-70.

Tamura, R. (2006). Human capital and economic development. *Journal of Development Economics, 79 (1),* 26-72.

Theft Act, 1978. Chapter 31, Section 16 (2), UK Laws

Thomas, A. R., & Gibson, K. M. (2003, April). Management is responsible, too. *Journal of Accountancy,* 53-56.

Tipton, H. F., & Krause, M. (2006). *Information Security Management Handbook.* New York: CRC Press.

Transparency International. (2007). 2004 Integrity Award winners. Available at: http://www.transparency.org/news_room/in_focus/2007/whistleblowers [Accessed on 30 June 2011]

Transparency International. (2009). *Corruption Perceptions Index 2009.* Available at: http://www.transparency.org/policy_research/surveys_indices/cpi/2009/cpi_2009_table [Accessed on 15 September 2010]

Transparency International. (2010). *2010 Corruption Perceptions Index.* The Global Coalition Against Corruption. Available at: http://www.transparency.org/policy_research/surveys_indices/cpi/2010/results [Accessed on 16 July 2011)

Trochim, W. K. (2006). *Types of reliability.* Retrieved from Research Methods Knowledge Base: http://www.socialresearchmethods.net/kb/reltypes.php [Accessed on

Trochim, W. K., & O'Donnelly, J. P. (2006). *The research methods knowledge base* (3rd ed.). New York: Thomson.

Turana, J. (2011). *Kenya FI's ride on Technology Wave*. Financial Technology. Available at: http://www.financialtechnologyafrica.com/ROI_Race.htm?reload=true [Accessed on 18 July 2011]

UNDP (n.d), Government Portal Assessment. Available at: http://www.gaportal.org/how-to/develop-governance-database/challenges-developing-national-governance-database [Accessed on 1 August 2011]

Utrero-González, N. (2007). Banking regulation, institutional framework and capital structure: International evidence from industry data . *The Quarterly Review of Economics and Finance*, *47* (4), 481-506.

Uzun, H., Szewczyk, S. H., & Varma, R. (2004). Board composition and corporate fraud. *Financial Analysts Journal, 60 (3),* 33– 43.

Van Dijk, J. J., & Terlouw, G. J. (1996). An international perspective of the business community as victims of fraud and crime. Security Journal , 7, 157-167.

Vanasco, R.R. (1998). Fraud Auditing. *Managerial Auditing Journal,* 19 *(1)* 4-71.

Vaughan, D. (2001). Transaction systems and unlawful organisational behaviour. In Shover, N. & Wright, J.P (Eds), *Crimes of Privilege: Readings in White Collar Crime,* 136-144. Oxford, UK: Oxford University Press.

Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: A case study. *Information Management and Computer Security, 16 (4),* 415-430.

Vincent, R. C., Bergiel, B. J., & Balsmeier, P. (2004). Effects of the electronic Nigerian money fraud on the brand equity of Nigeria and Africa. *Management Research News, 27 (6),* 11-20.

Vinten, G. (1994). Whistleblowing – *Subversion or corporate Citizenship?* New York: St. Martin's Press.

Wafula, P. (2010). *New Agency Banking System Deepens Access to Financial Services.* Financial Technology. Available at:

http://www.financialtechnologyafrica.com/New_Agency_Banking.html [Accessed on 21 June 2011]

Wallace, W. A. (2004). The economic role of the audit in free and regulated markets: A look back and a look forward. *Research in Accounting Regulation, 17*, 267-298.

Watson, W. (1990). Types of pluralism. *The Monist, 73*(3), 350–367.

Watson, D. M. (2003). Cultural dynamics of corporate fraud. Cross Cultural Management: An International Journal, 10 (1), 40-54.

Waweru, N.M. and Kalani, V.M (2009). Commercial Banking Crises In Kenya: Causes and remedies. *African Journal of Accounting, Economics, Finance and Banking Research, 4 (4)*, 12-33.

Webster (1997, 1976, 1941). Webster's New Collegiate Dictionary.

Weisburd, D., Waring, E., Chayet, E. (2001). *White collar crime and criminal careers*. New York: Cambridge University Press.

Weiss, J. W. (2009). Business ethics: A stakeholder and issues management approach. 5th ed. Cincinatti, Ohio: Cengage Learning.

Wells, J. (2007). *Corporate fraud handbook: Prevention and detection* (2nd ed.). London: John Wiley and Sons.

Wells, J.T. (2005). *Principles of fraud examination*. London: John Wiley and Sons.

Wells, J. T. (2004). New approaches to fraud deterrence. *Journal of Accountancy, 197 (2)*, 72-76.

Westernhagen, N., Harada, E., Nagata, T., Vale, B., Ayuso, J., Saurina, J. (2004). *Bank failures in mature economies.* Basel Committee on Banking Supervision. Basel, Switzerland: Bank for International Settlements.

Wheeler, R., & Aitkin, A. (2000). Multiple algorithms for fraud detection. *Knowledge Based Systems, 13*, 93-99.

Wheeler, S., Weisburd, D., & Bode, N. (1988). White-collar crimes and criminals. *American Criminal Law Review, 25:* 331 – 357.

Wickramasinghe, D., & Hopper, T. (2005). A cultural political economy of management accounting controls: a case study of a textile Mill in a traditional Sinhalese village. Critical Perspectives on Accounting, 16 (4), 473-503.

Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. *Journal of Economic Crime Management, 2* (2).

Wilson, J.O., Casu, B., Girardone, C., Molyneux, P. (2010). Emerging themes in banking: Recent literature and directions for future research. *The British Accounting Review*, 42, 153-169

Winkler, A. (2004). Corporate law or the law of business? Stakeholders and corporate governance at the end of history. *Law and Contemporary Problems, 67* (4), 109-133.

Wolfe, D.T., and Hermanson, D.R. (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *CPA Journal* 74(12)(Dec): 38-42.

Zagaris, B. (2010). *International white collar crime.* Cambridge: Cambridge University Press.

Zahra, S. A., Priem, R. L., & Rasheed, A. A. (2007). Understanding the causes and effects of top management fraud. *Organisational Dynamics, 36 (2),* 122-139.

Zhao, T., Casu, B., & Ferrari, A. (2009). *Competition and risk taking incentives in the lending market: An application to Indian banking*. Centre for Banking Research Working Papers, WP-CBR-02-2009. Cass Business School, City University London.

Zhao, T., Casu, B., & Ferrari, A. (2010). The impact of regulatory reforms on cost structure, ownership and competition in Indian Banking. *Journal of Banking and Finance, 34,* 246-254

Appendix I Statistical Outcomes

I.A Cross tabulations by Organisational Description

8.7.1 Views on Fraud

			Description of the operation of your institutions					
			Loc. bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Classification of fraud problem	Major Problem	Count	17	8	17	2	10	54
		% of Total	28.3%	13.3%	28.3%	3.3%	16.7%	90.0%
	Minor Problem	Count	2	0	2	0	1	5
		% of Total	3.3%	.0%	3.3%	.0%	1.7%	8.3%
	Not a Problem	Count	0	0	0	0	1	1
		% of Total	.0%	.0%	.0%	.0%	1.7%	1.7%
	Total	Count	19	8	19	2	12	60
		% of Total	31.7%	13.3%	31.7%	3.3%	20.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Intern. bank	Intern Sub	Reg. Bank	Total
Likelihood of frauds in financial sector	Very likely	Count	12	4	15	1	9	41
		% within Description of the operation of your institutions	63.2%	50.0%	78.9%	50.0%	75.0%	68.3%
	Quite likely	Count	3	3	2	1	3	12
		% within Description of the operation of your institutions	15.8%	37.5%	10.5%	50.0%	25.0%	20.0%
	Likely	Count	3	1	2	0	0	6
		% within Description of the operation of your institutions	15.8%	12.5%	10.5%	.0%	.0%	10.0%
	Quite unlikely	Count	1	0	0	0	0	1
		% within Description of the operation of your institutions	5.3%	.0%	.0%	.0%	.0%	1.7%
	Total	Count	19	8	19	2	12	60
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Opinion on overall trend of fraud	Increasingly Rapidly	Count	3	2	7	0	0	12
		% within Description of the operation of your institutions	15.8%	25.0%	36.8%	.0%	.0%	20.0%
	Increasing	Count	13	4	9	2	10	38
		% within Description of the operation of your institutions	68.4%	50.0%	47.4%	100.0%	83.3%	63.3%
	Constant	Count	2	2	2	0	1	7
		% within Description of the operation of your institutions	10.5%	25.0%	10.5%	.0%	8.3%	11.7%
	Decreasing	Count	1	0	1	0	1	3
		% within Description of the operation of your institutions	5.3%	.0%	5.3%	.0%	8.3%	5.0%
	Total	Count	19	8	19	2	12	60
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

8.7.2 Characteristics of the Fraud Experience

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Main perpetrator of the fraud	An internal perpetrator working alone	Count	2	0	2	0	1	5
		% within Description of the operation of your institutions	10.5%	.0%	10.5%	.0%	8.3%	8.3%
	Collusion between internal perpetrators	Count	4	0	3	0	1	8
		% within Description of the operation of your institutions	21.1%	.0%	15.8%	.0%	8.3%	13.3%
	An external perpetrator working alone	Count	1	0	1	0	0	2
		% within Description of the operation of your institutions	5.3%	.0%	5.3%	.0%	.0%	3.3%
	Collusion between external perpetrators	Count	1	0	1	0	1	3
		% within Description of the operation of your institutions	5.3%	.0%	5.3%	.0%	8.3%	5.0%
	Colluding internal and external perpetrators	Count	11	8	12	2	9	42
		% within Description of the operation of your institutions	57.9%	100.0%	63.2%	100.0%	75.0%	70.0%
	Total	Count	19	8	19	2	12	60
		% within Description of operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Internal 1st party	An Executive (Director/Officer)	Count	1	0	0	1	0	2
		% within Description of the operation of your institutions	5.9%	.0%	.0%	50.0%	.0%	3.7%
	A junior manager	Count	0	2	0	0	3	5
		% within Description of the operation of your institutions	.0%	28.6%	.0%	.0%	27.3%	9.3%
	A middle manager	Count	5	0	2	0	2	9
		% within Description of the operation of your institutions	29.4%	.0%	11.8%	.0%	18.2%	16.7%
	A senior manager	Count	2	0	3	0	1	6
		% within Description of the operation of your institutions	11.8%	.0%	17.6%	.0%	9.1%	11.1%
	A junior non-managerial employee	Count	4	3	7	0	4	18
		% within Description of the operation of your institutions	23.5%	42.9%	41.2%	.0%	36.4%	33.3%
	A middle non-managerial employee	Count	3	2	2	1	0	8
		% within Description of the operation of your institutions	17.6%	28.6%	11.8%	50.0%	.0%	14.8%

	A supervisor	Count	2	0	3	0	1	6
		% within Description of the operation of your institutions	11.8%	.0%	17.6%	.0%	9.1%	11.1%
	Total	Count	17	7	17	2	11	54
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Internal 2nd party	An owner	Count	0	0	0	1	0	1
		% within Description of the operation of your institutions	.0%	.0%	.0%	50.0%	.0%	3.0%
	An Executive (Director/Officer)	Count	1	0	0	0	0	1
		% within Description of the operation of your institutions	9.1%	.0%	.0%	.0%	.0%	3.0%
	A junior manager	Count	4	0	3	0	2	9
		% within Description of the operation of your institutions	36.4%	.0%	25.0%	.0%	40.0%	27.3%
	A middle manager	Count	0	0	3	0	0	3
		% within Description of the operation of your institutions	.0%	.0%	25.0%	.0%	.0%	9.1%
	A senior manager	Count	1	0	0	0	1	2
		% within Description of the operation of your institutions	9.1%	.0%	.0%	.0%	20.0%	6.1%
	A junior non-managerial employee	Count	2	0	3	0	1	6
		% within Description of the operation of your institutions	18.2%	.0%	25.0%	.0%	20.0%	18.2%

	A middle non-managerial employee	Count	1	0	2	0	1	4
		% within Description of the operation of your institutions	9.1%	.0%	16.7%	.0%	20.0%	12.1%
	A supervisor	Count	2	3	1	1	0	7
		% within Description of the operation of your institutions	18.2%	100.0%	8.3%	50.0%	.0%	21.2%
	Total	Count	11	3	12	2	5	33
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
External 1st Party	A Customer	Count	8	3	3	1	5	20
		% within Description of the operation of your institutions	57.1%	37.5%	20.0%	50.0%	45.5%	40.0%
	A competitor	Count	0	0	1	0	0	1
		% within Description of the operation of your institutions	.0%	.0%	6.7%	.0%	.0%	2.0%
	A supplier	Count	0	1	1	1	0	3
		% within Description of the operation of your institutions	.0%	12.5%	6.7%	50.0%	.0%	6.0%
	A Contractor	Count	1	0	0	0	1	2
		% within Description of the operation of your institutions	7.1%	.0%	.0%	.0%	9.1%	4.0%
	A former Employee	Count	1	2	1	0	2	6
		% within Description of the operation of your institutions	7.1%	25.0%	6.7%	.0%	18.2%	12.0%
	An organised Criminal	Count	4	0	6	0	3	13
		% within Description of the operation of your institutions	28.6%	.0%	40.0%	.0%	27.3%	26.0%

	A company agent	Count	0	0	3	0	0	3
		% within Description of the operation of your institutions	.0%	.0%	20.0%	.0%	.0%	6.0%
	A Friend	Count	0	2	0	0	0	2
		% within Description of the operation of your institutions	.0%	25.0%	.0%	.0%	.0%	4.0%
	Total	Count	14	8	15	2	11	50
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Main perpetrator of the fraud	An internal perpetrator working alone	Count	2	0	2	0	1	5
		% within Description of the operation of your institutions	10.5%	.0%	10.5%	.0%	8.3%	8.3%
	Collusion between internal perpetrators	Count	4	0	3	0	1	8
		% within Description of the operation of your institutions	21.1%	.0%	15.8%	.0%	8.3%	13.3%
	An external perpetrator working alone	Count	1	0	1	0	0	2
		% within Description of the operation of your institutions	5.3%	.0%	5.3%	.0%	.0%	3.3%
	Collusion between external perpetrators	Count	1	0	1	0	1	3
		% within Description of the operation of your institutions	5.3%	.0%	5.3%	.0%	8.3%	5.0%
	Colluding internal and external perpetrators	Count	11	8	12	2	9	42
		% within Description of the operation of your institutions	57.9%	100.0%	63.2%	100.0%	75.0%	70.0%
	Total	Count	19	8	19	2	12	60
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
External 2nd Party	A Customer	Count	0	2	3	0	2	7
		% within Description of the operation of your institutions	.0%	50.0%	33.3%	.0%	25.0%	25.9%
	A competitor	Count	0	0	1	0	0	1
		% within Description of the operation of your institutions	.0%	.0%	11.1%	.0%	.0%	3.7%
	A supplier	Count	0	0	1	1	2	4
		% within Description of the operation of your institutions	.0%	.0%	11.1%	50.0%	25.0%	14.8%
	A former Employee	Count	1	0	0	0	0	1
		% within Description of the operation of your institutions	25.0%	.0%	.0%	.0%	.0%	3.7%
	An organised Criminal	Count	3	1	3	1	2	10
		% within Description of the operation of your institutions	75.0%	25.0%	33.3%	50.0%	25.0%	37.0%
	A company agent	Count	0	0	1	0	1	2
		% within Description of the operation of your institutions	.0%	.0%	11.1%	.0%	12.5%	7.4%

	Other	Count	0	1	0	0	1	2
		% within Description of the operation of your institutions	.0%	25.0%	.0%	.0%	12.5%	7.4%
	Total	Count	4	4	9	2	8	27
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Age of the Internal 1st Party	Below 30yrs	Count	3	2	8	1	5	19
		% within Description of the operation of your institutions	17.6%	25.0%	50.0%	50.0%	45.5%	35.2%
	31-40yrs	Count	11	6	6	0	5	28
		% within Description of the operation of your institutions	64.7%	75.0%	37.5%	.0%	45.5%	51.9%
	41-50yrs	Count	3	0	2	0	1	6
		% within Description of the operation of your institutions	17.6%	.0%	12.5%	.0%	9.1%	11.1%
	Over 50yrs	Count	0	0	0	1	0	1
		% within Description of the operation of your institutions	.0%	.0%	.0%	50.0%	.0%	1.9%
	Total	Count	17	8	16	2	11	54
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Gender of Internal 1st Party	Male	Count	14	5	15	2	7	43
		% within Description of the operation of your institutions	82.4%	62.5%	88.2%	100.0%	63.6%	78.2%
	Female	Count	3	3	2	0	4	12
		% within Description of the operation of your institutions	17.6%	37.5%	11.8%	.0%	36.4%	21.8%
	Total	Count	17	8	17	2	11	55
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Intern. Sub.	Reg. Bank	Total
Age of the Internal 2nd Party	Below 30yrs	Count	5	1	2	1	0	9
		% within Description of the operation of your institutions	45.5%	33.3%	16.7%	50.0%	.0%	27.3%
	31-40yrs	Count	4	2	10	0	5	21
		% within Description of the operation of your institutions	36.4%	66.7%	83.3%	.0%	100.0%	63.6%
	41-50yrs	Count	2	0	0	0	0	2
		% within Description of the operation of your institutions	18.2%	.0%	.0%	.0%	.0%	6.1%
	Over 50yrs	Count	0	0	0	1	0	1
		% within Description of the operation of your institutions	.0%	.0%	.0%	50.0%	.0%	3.0%
	Total	Count	11	3	12	2	5	33
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Intern. bank	Intern. Sub.	Reg. Bank	Total
Gender of the Internal 2nd Party	Male	Count	8	2	8	2	3	23
		% within Description of the operation of your institutions	72.7%	66.7%	61.5%	100.0%	60.0%	67.6%
	Female	Count	3	1	5	0	2	11
		% within Description of the operation of your institutions	27.3%	33.3%	38.5%	.0%	40.0%	32.4%
	Total	Count	11	3	13	2	5	34
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Intern. Sub.	Reg. Bank	Total
Age of the External 1st Party	Below 30yrs	Count	1	2	2	0	2	7
		% within Description of the operation of your institutions	7.7%	25.0%	14.3%	.0%	20.0%	14.9%
	31-40yrs	Count	9	5	7	2	7	30
		% within Description of the operation of your institutions	69.2%	62.5%	50.0%	100.0%	70.0%	63.8%
	41-50yrs	Count	3	1	4	0	1	9
		% within Description of the operation of your institutions	23.1%	12.5%	28.6%	.0%	10.0%	19.1%
	Over 50yrs	Count	0	0	1	0	0	1
		% within Description of the operation of your institutions	.0%	.0%	7.1%	.0%	.0%	2.1%
	Total	Count	13	8	14	2	10	47
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Intern. bank	Intern. Sub.	Reg. Bank	Total
Gender of External 1st Party	Below 30yrs	Count	13	8	13	2	8	44
		% within Description of the operation of your institutions	92.9%	100.0%	86.7%	100.0%	80.0%	89.8%
	31-40yrs	Count	1	0	2	0	2	5
		% within Description of the operation of your institutions	7.1%	.0%	13.3%	.0%	20.0%	10.2%
	Total	Count	14	8	15	2	10	49
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Age of the External 2nd Party	Below 30yrs	Count	0	2	0	0	0	2
		% within Description of the operation of your institutions	.0%	50.0%	.0%	.0%	.0%	7.7%
	31-40yrs	Count	4	2	6	2	8	22
		% within Description of the operation of your institutions	100.0%	50.0%	75.0%	100.0%	100.0%	84.6%
	41-50yrs	Count	0	0	1	0	0	1
		% within Description of the operation of your institutions	.0%	.0%	12.5%	.0%	.0%	3.8%
	Over 50yrs	Count	0	0	1	0	0	1
		% within Description of the operation of your institutions	.0%	.0%	12.5%	.0%	.0%	3.8%
	Total	Count	4	4	8	2	8	26
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Gender of the External 2nd Party	Below 30yrs	Count	4	3	7	2	6	22
		% within Description of the operation of your institutions	100.0%	75.0%	77.8%	100.0%	75.0%	81.5%
	31-40yrs	Count	0	1	2	0	2	5
		% within Description of the operation of your institutions	.0%	25.0%	22.2%	.0%	25.0%	18.5%
	Total	Count	4	4	9	2	8	27
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

8.7.3 Software and Fraud Detection Methods in Use

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Password protection in use	Yes	Count	17	8	19	2	12	58
		Expected Count	17.0	8.0	19.0	2.0	12.0	58.0
		% within Password protection in use	29.3%	13.8%	32.8%	3.4%	20.7%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	29.3%	13.8%	32.8%	3.4%	20.7%	100.0%
	Total	Count	17	8	19	2	12	58
		Expected Count	17.0	8.0	19.0	2.0	12.0	58.0
		% within Password protection in use	29.3%	13.8%	32.8%	3.4%	20.7%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	29.3%	13.8%	32.8%	3.4%	20.7%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Antivirus software in use	Yes	Count	18	8	19	2	12	59
		Expected Count	18.0	8.0	19.0	2.0	12.0	59.0
		% within Antivirus software in use	30.5%	13.6%	32.2%	3.4%	20.3%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	30.5%	13.6%	32.2%	3.4%	20.3%	100.0%
	Total	Count	18	8	19	2	12	59
		Expected Count	18.0	8.0	19.0	2.0	12.0	59.0
		% within Antivirus software in use	30.5%	13.6%	32.2%	3.4%	20.3%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	30.5%	13.6%	32.2%	3.4%	20.3%	100.0%

			Description of the operation of your institutions				
			Local bank	Nat. Bank	Inter. bank	Reg. Bank	Total
Firewall software in use	Yes	Count	12	2	8	3	25
		Expected Count	12.0	2.0	8.0	3.0	25.0
		% within Firewall software in use	48.0%	8.0%	32.0%	12.0%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	48.0%	8.0%	32.0%	12.0%	100.0%
	Total	Count	12	2	8	3	25
		Expected Count	12.0	2.0	8.0	3.0	25.0
		% within Firewall software in use	48.0%	8.0%	32.0%	12.0%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	48.0%	8.0%	32.0%	12.0%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Discovery sampling in use	Yes	Count	3	3	10	1	7	24
		Expected Count	3.0	3.0	10.0	1.0	7.0	24.0
		% within Discovery sampling in use	12.5%	12.5%	41.7%	4.2%	29.2%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	12.5%	12.5%	41.7%	4.2%	29.2%	100.0%
	Total	Count	3	3	10	1	7	24
		Expected Count	3.0	3.0	10.0	1.0	7.0	24.0
		% within Discovery sampling in use	12.5%	12.5%	41.7%	4.2%	29.2%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	12.5%	12.5%	41.7%	4.2%	29.2%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Ratio analysis in use	Yes	Count	6	2	6	1	3	18
		Expected Count	6.0	2.0	6.0	1.0	3.0	18.0
		% within Ratio analysis in use	33.3%	11.1%	33.3%	5.6%	16.7%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	33.3%	11.1%	33.3%	5.6%	16.7%	100.0%
	Total	Count	6	2	6	1	3	18
		Expected Count	6.0	2.0	6.0	1.0	3.0	18.0
		% within Ratio analysis in use	33.3%	11.1%	33.3%	5.6%	16.7%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	33.3%	11.1%	33.3%	5.6%	16.7%	100.0%

			Description of the operation of your institutions			
			Local bank	Inter. bank	Reg. Bank	Total
Digital analysis in use	Yes	Count	2	7	1	10
		Expected Count	2.0	7.0	1.0	10.0
		% within Digital analysis in use	20.0%	70.0%	10.0%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%
		% of Total	20.0%	70.0%	10.0%	100.0%
	Total	Count	2	7	1	10
		Expected Count	2.0	7.0	1.0	10.0
		% within Digital analysis in use	20.0%	70.0%	10.0%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%
		% of Total	20.0%	70.0%	10.0%	100.0%

			Description of the operation of your institutions				
			Local bank	Nat. Bank	Inter. bank	Reg. Bank	Total
Data mining software in use	Yes	Count	4	1	9	8	22
		Expected Count	4.0	1.0	9.0	8.0	22.0
		% within Data mining software in use	18.2%	4.5%	40.9%	36.4%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	18.2%	4.5%	40.9%	36.4%	100.0%
	Total	Count	4	1	9	8	22
		Expected Count	4.0	1.0	9.0	8.0	22.0
		% within Data mining software in use	18.2%	4.5%	40.9%	36.4%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	18.2%	4.5%	40.9%	36.4%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Filtering software in use	Yes	Count	12	4	12	2	8	38
		Expected Count	12.0	4.0	12.0	2.0	8.0	38.0
		% within Filtering software in use	31.6%	10.5%	31.6%	5.3%	21.1%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	31.6%	10.5%	31.6%	5.3%	21.1%	100.0%
	Total	Count	12	4	12	2	8	38
		Expected Count	12.0	4.0	12.0	2.0	8.0	38.0
		% within Filtering software in use	31.6%	10.5%	31.6%	5.3%	21.1%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	31.6%	10.5%	31.6%	5.3%	21.1%	100.0%

			Description of the operation of your institutions					
			Local bank	Nat. Bank	Inter. bank	Inter. Sub.	Reg. Bank	Total
Continuous Auditing software in use	Yes	Count	14	7	14	1	10	46
		Expected Count	14.0	7.0	14.0	1.0	10.0	46.0
		% within Continuous Auditing software in use	30.4%	15.2%	30.4%	2.2%	21.7%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	30.4%	15.2%	30.4%	2.2%	21.7%	100.0%
	Total	Count	14	7	14	1	10	46
		Expected Count	14.0	7.0	14.0	1.0	10.0	46.0
		% within Continuous Auditing software in use	30.4%	15.2%	30.4%	2.2%	21.7%	100.0%
		% within Description of the operation of your institutions	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
		% of Total	30.4%	15.2%	30.4%	2.2%	21.7%	100.0%

I.B T-Tests

8.7.4 Rankings of Fraud Prevention Measures

	No of employees	N	Mean	Std. Deviation	Std. Error Mean
Improvement or review of internal controls	>= 4	21	1.90	1.044	.228
	< 4	34	1.29	.871	.149
Establishing fraud prevention policies	>= 4	17	2.71	1.160	.281
	< 4	20	2.85	1.268	.284
Establishing an ethical code of conduct	>= 4	10	3.20	1.476	.467
	< 4	15	3.40	1.183	.306
Implementing a fraud hotline	>= 4	8	4.25	.707	.250
	< 4	15	3.27	.799	.206
Training employees on fraud prevention	>= 4	20	2.65	1.348	.302
	< 4	24	2.83	1.049	.214
Screening/reference checks on new employees	>= 4	8	3.50	1.414	.500
	< 4	13	3.00	1.291	.358
Establishing a fraud budget	>= 4	2	3.00	2.828	2.000
	< 4	2	2.50	2.121	1.500
Automated fraud prevention	>= 4	5	4.60	.894	.400
	< 4	6	3.50	1.378	.563
Staff rotation policy	>= 4	5	4.20	.837	.374
	< 4	11	4.18	.874	.263
Security department	>= 4	6	3.50	1.761	.719
	< 4	5	3.60	1.140	.510
Ethics training	>= 4	1	4.00	.	.
	< 4	5	3.80	1.095	.490
Use of forensic accountants	>= 4	2	2.00	.000	.000
	< 4	2	2.50	.707	.500
Close supervision	>= 4	0[a]	.	.	.
	< 4	10	4.10	1.101	.348
Fraud auditing	>= 4	3	4.00	1.000	.577
	< 4	3	4.67	.577	.333
Inventory observation	>= 4	0[a]	.	.	.
	< 4	1	5.00	.	.
Surveillance of electronic correspondence	>= 4	0[a]	.	.	.
	< 4	1	2.00	.	.

Limiting opportunities	>= 4	4	2.75	1.708	.854
	< 4	3	4.00	1.732	1.000
High deterrence measures	>= 4	3	2.67	1.528	.882
	< 4	2	4.00	1.414	1.000
Spot checking	>= 4	4	3.75	1.258	.629
	< 4	6	4.33	.816	.333
Asset protection programs	>= 4	0[a]	.	.	.
	< 4	0[a]	.	.	.
a. t cannot be computed because at least one of the groups is empty.					

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Improvement or review of internal controls	Equal variances assumed	3.924	.053	2.340	53	.023	.611	.261	.087	1.134
	Equal variances not assumed			2.241	36.780	.031	.611	.273	.058	1.163
Establishing fraud prevention policies	Equal variances assumed	.284	.598	-.358	35	.722	-.144	.402	-.961	.673
	Equal variances not assumed			-.361	34.787	.720	-.144	.399	-.955	.667
Establishing an ethical code of conduct	Equal variances assumed	.412	.527	-.375	23	.711	-.200	.533	-1.303	.903
	Equal variances not assume			-.359	16.428	.724	-.200	.558	-1.380	.980

	d									
Implementing a fraud hotline	Equal variances assumed	.095	.760	2.919	21	.008	.983	.337	.283	1.684
	Equal variances not assumed			3.034	16.053	.008	.983	.324	.296	1.670
Training employees on fraud prevention	Equal variances assumed	2.445	.125	-.507	42	.615	-.183	.362	-.913	.546
	Equal variances not assumed			-.496	35.541	.623	-.183	.370	-.934	.567
Screening/reference checks on new employees	Equal variances assumed	.965	.338	.832	19	.416	.500	.601	-.758	1.758
	Equal variances not assumed			.813	13.890	.430	.500	.615	-.820	1.820
Establishing a fraud budget	Equal variances assumed	.	.	.200	2	.860	.500	2.500	-10.257	11.257
	Equal variances not assume			.200	1.855	.861	.500	2.500	-11.107	12.107

	d									
Automated fraud prevention	Equal variances assumed	2.739	.132	1.529	9	.161	1.100	.719	-.527	2.727
	Equal variances not assumed			1.593	8.588	.147	1.100	.690	-.473	2.673
Staff rotation policy	Equal variances assumed	.225	.642	.039	14	.969	.018	.466	-.981	1.017
	Equal variances not assumed			.040	8.149	.969	.018	.458	-1.034	1.070
Security department	Equal variances assumed	2.835	.127	-.109	9	.916	-.100	.918	-2.177	1.977
	Equal variances not assumed			-.113	8.582	.912	-.100	.881	-2.109	1.909
Ethics training	Equal variances assumed	.	.	.167	4	.876	.200	1.200	-3.132	3.532
	Equal variances not assume			.	.	.	.200	.	.	.

	d									
Use of forensic accountants	Equal variances assumed	.	.	-1.000	2	.423	-.500	.500	-2.651	1.651
	Equal variances not assumed			-1.000	1.000	.500	-.500	.500	-6.853	5.853
Fraud auditing	Equal variances assumed	.400	.561	-1.000	4	.374	-.667	.667	-2.518	1.184
	Equal variances not assumed			-1.000	3.200	.387	-.667	.667	-2.715	1.382
Limiting opportunities	Equal variances assumed	.019	.896	-.953	5	.384	-1.250	1.312	-4.622	2.122
	Equal variances not assumed			-.951	4.415	.391	-1.250	1.315	-4.769	2.269
High deterrence measures	Equal variances assumed	.046	.844	-.980	3	.399	-1.333	1.361	-5.664	2.997
	Equal variances not assume			-1.000	2.427	.406	-1.333	1.333	-6.204	3.538

	d									
Spot checking	Equal variances assumed	.354	.568	-.899	8	.395	-.583	.649	-2.080	.913
	Equal variances not assumed			-.819	4.698	.452	-.583	.712	-2.449	1.283

I.C Hypotheses variables

8.7.5 Variables extracted from the questionnaire item scores

Variable	Definition	Level	SPSS value labels for categories [a]
PERCENTAGE LOSS TO FRAUD	Overall monetary loss from fraud as a percentage of business turn-over	Ordinal	1 = Less than 1% 2 = More than 1%
VALUE LOSS TO FRAUD	Direct value of loss to the bank due to fraud (KES)	Ordinal	1 = Less than 5,000,000 2 = More than 5,000,000
PERCENTAGE TURNOVER LOSS TO FRAUD	Percentage of the bank's annual turnover lost to fraud	Ordinal	1 = Less than 1% 2 = More than 1%
TYPE OF BANK	Classification of bank	Nominal	1 = International or International Subsidiary 2 = National, Regional, or Local
SIZE OF BANK	Number of employees in the bank	Ordinal	1 = Less than 500 2 = More than 500
ACTION	Action taken by the bank when fraud was discovered	Nominal	1 = Criminal prosecution 2 = Civil prosecution for recovery
PARTY	Party involved in the fraud	Nominal	1 = Internal 1st Party 2 = Internal 2nd Party 3 = External 1st Party 4 = External 2nd Party
DETECTED FRAUD	How much fraud the bank detects as a percentage of the total incidences	Ordinal	1 = 75% or less 2 = More than 75%
SECURITY PROTOCOL	Measures taken by the bank to prevent fraud	Nominal	0 = No (not ranked 1 to 5) 1 = Yes (ranked 1 to 5)

[a] Note: The categories used for the statistical analysis were collapsed from the larger number of categories used in the questionnaire. Collapsing of categories was essential to ensure that at least 50% of the cells each cross-tabulations included 5 or more cases.

I.D Cross-tabulations of security protocols

8.7.6 Cross-tabulations of detected fraud vs. security protocols used

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Improvement or review of internal controls	No	2	2	4	2.008	.156
	Yes	10	41	51		
Total		12	27	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Establishing fraud prevention policies	No	5	14	19	.344	.557
	Yes	7	29	36		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Establishing an ethical code of conduct	No	8	25	33	.284	.594
	Yes	4	18	22		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Implementing a fraud hotline	No	5	30	35	3.201	.074
	Yes	7	13	20		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Training employees on fraud prevention	No	6	8	14	4.873	.027*
	Yes	6	35	41		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Screening/reference checks on new employees	No	10	26	36	2.170	.141
	Yes	2	17	19		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Establishing a fraud budget	No	9	43	52	11.370	.001*
	Yes	3	0	3		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Automated fraud prevention	No	11	38	49	.105	.746
	Yes	1	5	6		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Staff rotation policy	No	8	32	40	.284	.594
	Yes	4	11	15		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Security department	No	10	34	44	.107	.744
	Yes	2	9	11		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Ethics training	No	11	39	50	.011	.918
	Yes	1	4	5		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Use of forensic accountants	No	10	42	52	3.742	.053
	Yes	2	1	3		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Close supervision	No	8	38	46	3.230	.072
	Yes	4	5	9		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Fraud Auditing	No	12	39	51	1.204	.273
	Yes	0	4	4		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Inventory observation	No	12	42	54	.284	.594
	Yes	0	1	1		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Surveillance of electronic correspondence	No	11	43	54	3.650	.056
	Yes	1	0	1		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Limiting opportunities	No	10	38	48	.214	.643
	Yes	2	5	7		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
High deterrence measures	No	12	38	50	1.535	.215
	Yes	0	5	5		
Total		12	43	55		

SECURITY PROTOCOL		DETECTED FRAUD ≤ 75%	DETECTED FRAUD >75%	Total	χ^2 test statistic	p-value
Spot checking	No	10	35	45	.024	.878
	Yes	2	8	40		
Total		12	43	55		

8.7.7 Cross-tabulations of size of bank vs. security protocols used

SECURITY PROTOCOL		SIZE OF BANK < 500	SIZE OF BANK > 500	Total	χ^2 test statistic	p-value
Improvement or review of internal controls	No	2	3	5	.055	.814
	Yes	25	30	55		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK < 500	SIZE OF BANK > 500	Total	χ^2 test statistic	p-value
Establishing fraud prevention policies	No	12	11	23	.776	.379
	Yes	15	22	37		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK < 500	SIZE OF BANK > 500	Total	χ^2 test statistic	p-value
Establishing an ethical code of conduct	No	12	23	35	3.896	.048*
	Yes	15	10	25		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK < 500	SIZE OF BANK > 500	Total	χ^2 test statistic	p-value
Implementing a fraud hotline	No	19	18	37	1.573	.210
	Yes	8	15	23		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK < 500	SIZE OF BANK > 500	Total	χ^2 test statistic	p-value
Training employees on fraud prevention	No	10	6	16	2.700	.100
	Yes	17	27	44		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK < 500	SIZE OF BANK > 500	Total	χ^2 test statistic	p-value
Screening/reference checks on new employees	No	18	21	39	.060	.807
	Yes	9	12	21		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Establishing a fraud budget	No	25	31	56	.043	.835
	Yes	2	2	4		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Automated fraud prevention	No	22	30	52	1.142	.285
	Yes	5	3	8		
Total		27	33			

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Staff rotation policy	No	19	25	44	.220	.639
	Yes	8	8	16		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Security department	No	23	26	49	.406	.524
	Yes	4	7	11		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Ethics training	No	22	32	54	3.958	.047*
	Yes	5	1	5		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Use of forensic accountants	No	25	31	56	.043	.835
	Yes	2	2	4		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Close supervision	No	19	31	50	5.939	.015*
	Yes	8	2	10		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Fraud Auditing	No	25	29	54	.367	.545
	Yes	2	4	6		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Inventory observation	No	27	32	59	.832	.362
	Yes	0	1	1		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Surveillance of electronic correspondence	No	26	33	59	1.243	.265
	Yes	1	0	1		
Total		27	33	60		

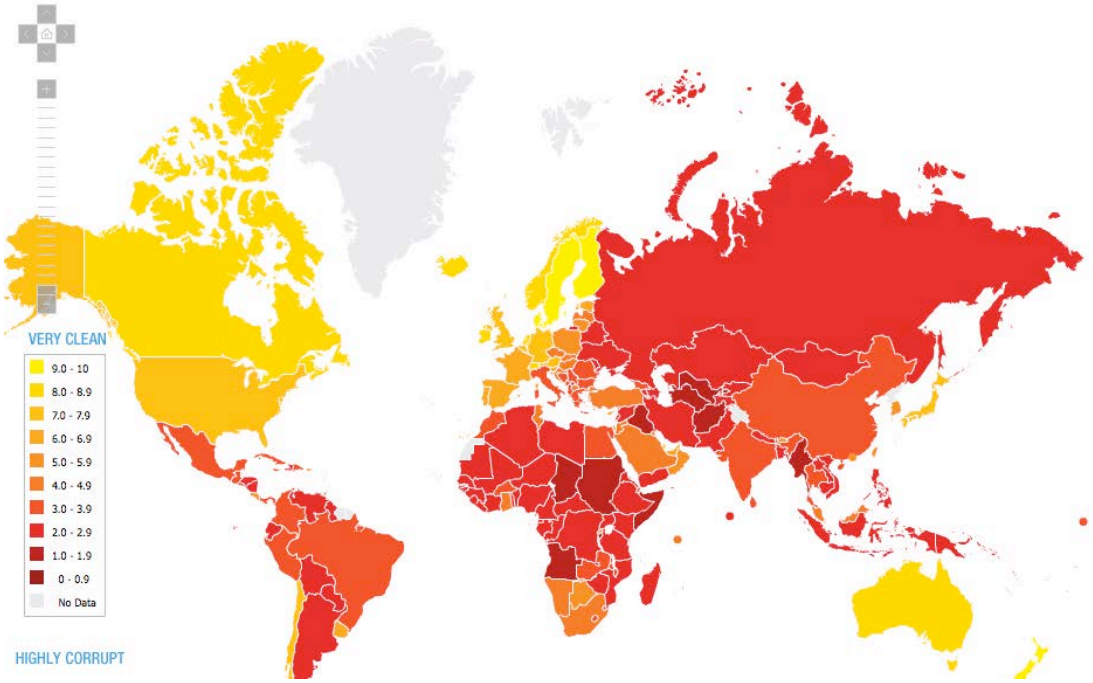
SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Limiting opportunities	No	25	28	53	.864	.353
	Yes	2	5	7		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
High deterrence measures	No	25	30	55	.055	.814
	Yes	2	3	5		
Total		27	33	60		

SECURITY PROTOCOL		SIZE OF BANK		Total	χ^2 test statistic	p-value
		< 500	> 500			
Spot checking	No	23	27	50	.121	.728
	Yes	4	6	10		
Total		27	33	60		

Appendix II Supporting Data

II.A. Corruption Perception Index, 2010



Source: Transparency International, 2010

II.B. CPI Rankings for Sub-Saharan Africa, 2010

SUB-SAHARAN AFRICA

RANK	REGIONAL RANK	COUNTRY / TERRITORY	CPI 2010 SCORE	90% CONFIDENCE INTERVAL		SURVEYS USED
				LOWER BOUND	UPPER BOUND	
33	1	Botswana	5.8	5.4	6.2	6
39	2	Mauritius	5.4	4.9	5.9	6
45	3	Cape Verde	5.1	4.1	6.1	4
49	4	Seychelles	4.8	3.0	6.8	3
54	5	South Africa	4.5	4.1	4.8	8
56	6	Namibia	4.4	3.9	4.9	6
62	7	Ghana	4.1	3.4	4.7	7
66	8	Rwanda	4.0	3.2	5.1	5
78	9	Lesotho	3.5	2.8	4.4	6
85	10	Malawi	3.4	2.8	3.9	7
87	11	Liberia	3.3	2.7	3.9	4
91	12	Gambia	3.2	1.9	4.4	5
91	12	Swaziland	3.2	3.1	3.4	4
98	14	Burkina Faso	3.1	2.4	3.8	6
101	15	Sao Tome and Principe	3.0	2.6	3.3	3
101	15	Zambia	3.0	2.7	3.3	7
105	17	Senegal	2.9	2.6	3.1	7
110	18	Benin	2.8	2.3	3.3	6
110	18	Gabon	2.8	2.1	3.3	3
116	20	Ethiopia	2.7	2.4	2.9	7
116	20	Mali	2.7	2.2	3.2	6
116	20	Mozambique	2.7	2.4	3.0	7
116	20	Tanzania	2.7	2.4	2.9	7
123	24	Eritrea	2.6	1.7	3.7	4
123	24	Madagascar	2.6	2.2	2.9	6
123	24	Niger	2.6	2.3	2.9	4
127	27	Uganda	2.5	2.1	2.9	7
134	28	Nigeria	2.4	2.2	2.7	7
134	28	Sierra Leone	2.4	2.1	2.6	5
134	28	Togo	2.4	1.8	3.0	4
134	28	Zimbabwe	2.4	1.8	3.0	7
143	32	Mauritania	2.3	1.9	2.7	6
146	33	Cameroon	2.2	2.0	2.4	7
146	33	Côte d'Ivoire	2.2	1.9	2.5	7

RANK	REGIONAL RANK	COUNTRY / TERRITORY	CPI 2010 SCORE	90% CONFIDENCE INTERVAL		SURVEYS USED
				LOWER BOUND	UPPER BOUND	
154	35	Central African Republic	2.1	2.0	2.3	4
154	35	Comoros	2.1	1.7	2.6	3
154	35	Congo-Brazzaville	2.1	1.9	2.3	5
154	35	Guinea-Bissau	2.1	2.0	2.1	3
154	35	Kenya	2.1	2.0	2.3	7
164	40	Democratic Republic of the Congo	2.0	1.7	2.3	4
164	40	Guinea	2.0	1.8	2.2	5
168	42	Angola	1.9	1.8	2.0	6
168	42	Equatorial Guinea	1.9	1.7	2.1	3
170	44	Burundi	1.8	1.6	2.0	6
171	45	Chad	1.7	1.6	1.9	6
172	46	Sudan	1.6	1.4	1.9	5
178	47	Somalia	1.1	0.9	1.4	3

Source: Transparency International, 2010

II.C. List of Commercial Banks in Kenya, 2008

1) African Banking Corporation Ltd
2) Bank of Africa Ltd
3) Bank of Baroda Ltd
4) Bank of India
5) Barclays Bank of Kenya Ltd
6) CFC Stanbic Bank Ltd
7) Charterhouse Bank Ltd (Bank under suspension by Central Bank of Kenya)
8) Chase Bank Ltd
9) Citibank, N.A.
10) City Finance Bank Ltd
11) Commercial Bank of Africa Ltd
12) Consolidated Bank of Kenya Ltd
13) Co-operative Bank of Kenya Ltd
14) Credit Bank Ltd
15) Development Bank of Kenya Ltd
16) Diamond Trust Bank Ltd
17) Dubai Bank Ltd
18) Ecobank Ltd
19) Equatorial Commercial Bank Ltd
20) Equity Bank Ltd
21) Family Bank Ltd
22) Fidelity Commercial Bank Ltd
23) Fina Bank Ltd
24) First Community Bank Ltd (New bank)
25) Giro Commercial Bank Ltd
26) Guardian Bank Ltd
27) Gulf African Bank Ltd (New Bank)
28) Habib AG Zurich
29) Habib Bank Ltd
30) Imperial Bank Limited
31) Investment & Mortgages Bank
32) Kenya Commercial Bank Ltd
33) K-Rep Bank Ltd
34) Middle East Bank Ltd
35) National Bank of Kenya Ltd
36) NIC Bank Ltd
37) Oriental Commercial Bank Ltd
38) Paramount-Universal Bank Ltd
39) Prime Bank Ltd.
40) Southern Credit Banking Corp. Ltd
41) Standard Chartered Bank Ltd
42) Transnational Bank Ltd
43) Victoria Commercial Bank Ltd

Non Banking Financial Institutions

44) Housing Finance Co. of Kenya Ltd
45) Savings & Loan Ltd

Source: Central Bank of Kenya, Bank Supervision Annual Report, 2008.

II.D. Ownership Structures of Banks

I) INSTITUTIONS IN TERMS OF SHAREHOLDING

a) Foreign owned institutions

i) Foreign owned not locally incorporated

Bank of Africa (K) Ltd.
Bank of India
Citibank N.A. Kenya
Habib Bank A.G. Zurich
Habib Bank Ltd.

ii) Foreign owned, locally incorporated institutions (Partly owned by locals)

- Bank of Baroda (K) Ltd.
- Barclays Bank of Kenya Ltd.
- Diamond Trust Bank Kenya Ltd.
- K-Rep Bank Ltd.
- Standard Chartered Bank (K) Ltd.
- Ecobank Ltd.
- Gulf Africa Bank (K) Ltd.
- First Community Bank

iii) Foreign owned but locally incorporated institutions (Wholly owned subsidiary)

UBA Kenya Bank Limited

b) Institutions with Government participation

- Consolidated Bank of Kenya Ltd.
- Development Bank of Kenya Ltd.
- Housing Finance Ltd.
- Kenya Commercial Bank Ltd.
- National Bank of Kenya Ltd.
- CFC Stanbic Bank Ltd.

c) Institutions locally owned

- African Banking Corporation Ltd.
- City Finance Bank Ltd.
- Commercial Bank of Africa Ltd.
- Co-operative Bank of Kenya Ltd.

- Credit Bank Ltd.
- Charterhouse Bank Ltd.
- Chase Bank (K) Ltd.
- Dubai Bank Kenya Ltd.
- Equatorial Commercial Bank Ltd.
- Equity Bank Ltd.
- Family Bank Ltd.
- Fidelity Commercial Bank Ltd.
- Fina Bank Ltd.
- Giro Commercial Bank Ltd.
- Guardian Bank Ltd.
- Imperial Bank Ltd.
- Investment & Mortgages Bank Ltd.
- Middle East Bank (K) Ltd.
- NIC Bank Ltd.
- Oriental Commercial Bank Ltd.
- Paramount Universal Bank Ltd.
- Prime Bank Ltd.
- Southern Credit Banking Corporation Ltd.
- Trans-National Bank Ltd.
- Victoria Commercial Bank Ltd.

d) Institutions Listed on the NSE

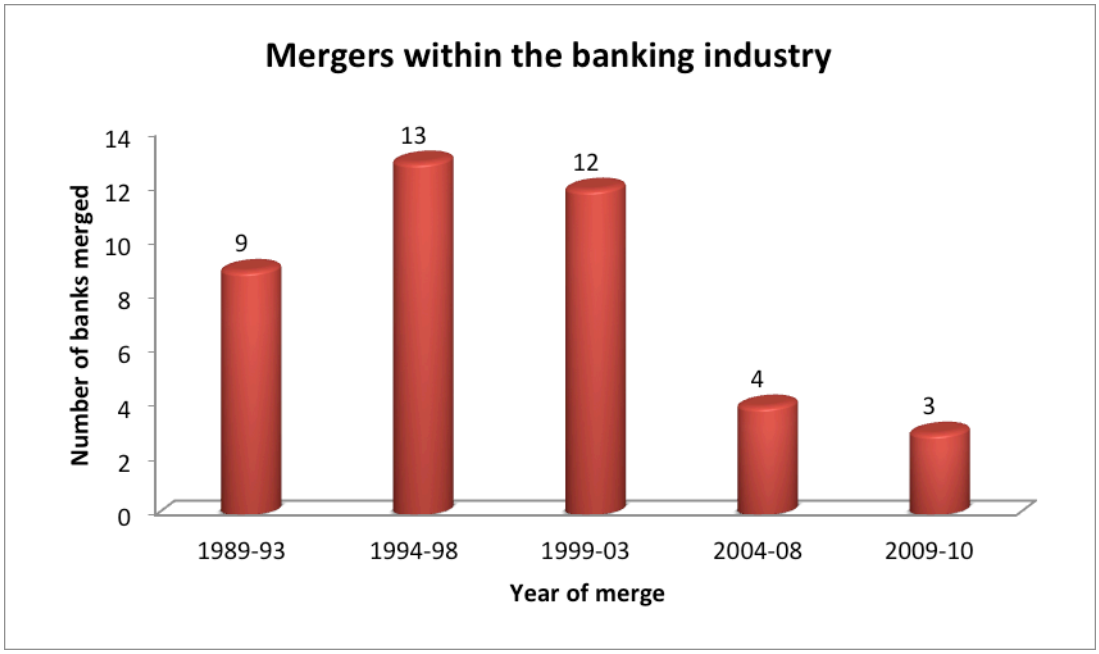
- Barclays Bank of Kenya Ltd.
- CFC Stanbic Bank Ltd.
- Equity Bank Ltd.
- Housing Finance Ltd.
- Kenya Commercial Bank Ltd.
- NIC Bank Ltd.
- Standard Chartered Bank (K) Ltd.
- Diamond Trust Bank Kenya Ltd.
- National Bank of Kenya
- Co-operative Bank of Kenya Ltd.

Source: Central Bank of Kenya, 2008(c):
http://www.centralbank.go.ke/financialsystem/banks/shareholding.aspx

II.E. Mergers in the Kenyan banking sector, 1989-2010

No.	Institution	Merged with	Current Name	Date approved
1	9 Financial Institutions	All 9 Financial Institutions Merged together	Consolidated Bank of Kenya Ltd	1989
2	Indosuez Merchant Finance	Banque Indosuez	Credit Agricole Indosuez	10.11.1994
3	Transnational Finance Ltd.	Transnational Bank Ltd.	Transnational Bank Ltd.	28.11.1994
4	Ken Baroda Finance Ltd.	Bank of Baroda (K) Ltd.	Bank of Baroda (K) Ltd.	02.12.1994
5	First American Finance Ltd.	First American Bank Ltd.	First American Bank (K) Ltd.	05.09.1995
6	Bank of India	Bank of India Finance Ltd.	Bank of India (Africa) Ltd.	15.11.1995
7	Stanbic Bank (K) Ltd.	Stanbic Finance (K) Ltd.	Stanbic Bank Kenya Ltd.	05.01.1996
8	Mercantile Finance Ltd.	Ambank Ltd.	Ambank Ltd.	15.01.1996
9	Delphis Finance Ltd.	Delphis Bank Ltd.	Delphis Bank Ltd.	17.01.1996
10	CBA Financial Services	Commercial Bank of Africa ltd	Commercial Bank of Africa ltd	26.01.1996
11	Trust Finance Ltd.	Trust Bank (K) Ltd.	Trust Bank (K) Ltd.	07.01.1997
12	National Industrial Credit Bank Ltd.	African Mercantile Banking Corp.	NIC Bank Ltd.	14.06.1997
13	Giro Bank Ltd.	Commerce Bank Ltd.	Giro Commercial Bank Ltd.	24.11.1998
14	Guardian Bank Ltd.	First National Finance Bank Ltd.	Guardian Bank Ltd.	24.11.1998
15	Diamond Trust Bank (K) Ltd.	Premier Savings & Finance Ltd.	Diamond Trust Bank (K) Ltd.	12.02.1999
16	National Bank of Kenya Ltd.	Kenya National Capital Corp.	National Bank of Kenya Ltd.	24.05.1999
17	Standard Chartered Bank (K) Ltd.	Standard Chartered Financial Services	Standard Chartered Bank (K) Ltd.	17.11.1999
18	Barclays Bank of Kenya Ltd.	Barclays Merchant Finance Ltd.	Barclays Bank of Kenya Ltd.	22.11.1999
19	Habib A.G. Zurich	Habib Africa Bank Ltd.	Habib Bank A.G. Zurich	30.11.1999
20	Guilders Inter. Bank Ltd.	Guardian Bank Ltd.	Guardian Bank Ltd.	03.12.1999
21	Universal Bank Ltd.	Paramount Bank Ltd.	Paramount Universal Bank	11.01.2000
22	Kenya Commercial Bank	Kenya Commercial Finance Co.	Kenya Commercial Bank Ltd.	21.03.2001
23	Citibank NA	ABN Amro Bank Ltd.	Citibank NA	16.10.2001
24	Bullion Bank Ltd.	Southern Credit Banking Corp. Ltd.	Southern Credit Banking Corp. Ltd.	07.12.2001
25	Co-operative Merchant Bank ltd	Co-operative Bank ltd	Co-operative Bank of Kenya ltd	28.05.2002
26	Biashara Bank Ltd.	Investment & Mortgage Bank Ltd.	Investment & Mortgage Bank Ltd.	01.12.2002
27	First American Bank ltd	Commercial Bank of Africa	Commercial Bank of	01.07.2005

		ltd	Africa ltd	
28	East African Building Society	Akiba Bank ltd	EABS Bank ltd	31.10.2005
29	Prime Capital & Credit Ltd.	Prime Bank Ltd.	Prime Bank Ltd.	01.01.2008
30	CFC Bank Ltd.	Stanbic Bank Ltd.	CFC Stanbic Bank Ltd.	01.06.2008
31	Savings and Loan (K) Limited	Kenya Commercial Bank Limited	Kenya Commercial Bank Limited	01.02.2010
32	City Finance Bank Ltd.	Jamii Bora Kenya Ltd.	Jamii Bora Bank Ltd.	11.02.2010
33	Equatorial Commercial Bank Ltd	Southern Credit Banking Corporation Ltd	Equatorial Commercial Bank Ltd	01.06.2010



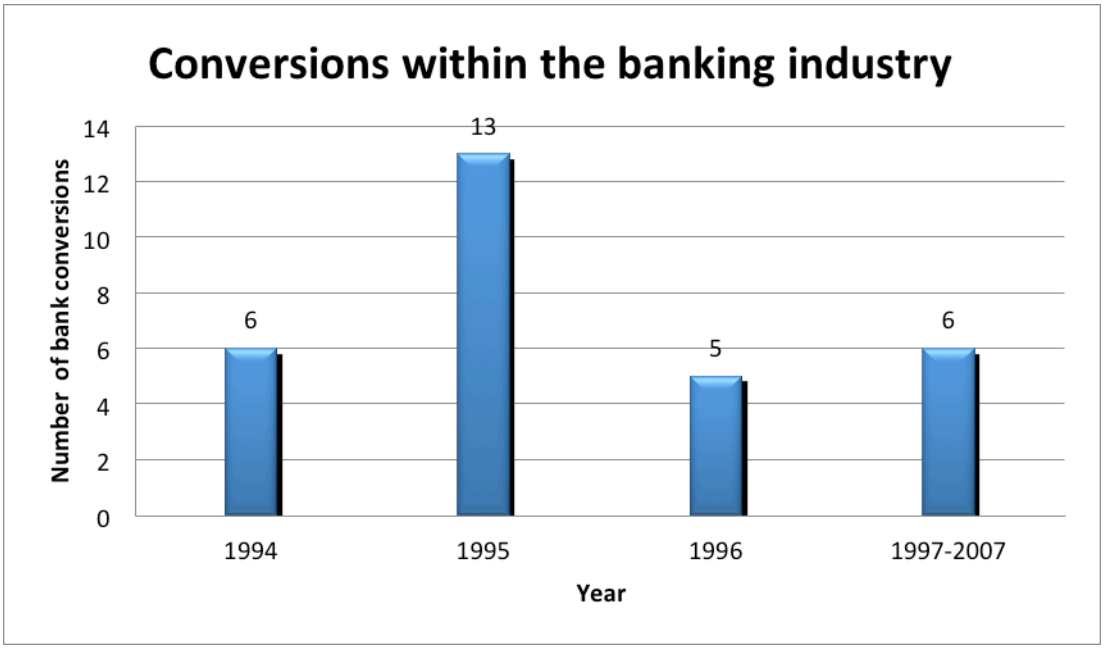
Mergers in the Kenyan Banking Industry
(Source: Adapted from Central Bank of Kenya, 2010)

Institution	Acquired by	Current Name	Date approved
Mashreq Bank Ltd.	Dubai Kenya Ltd.	Dubai Bank Ltd.	01.04.2000
Credit Agricole Indosuez (K) Ltd.	Bank of Africa Kenya Ltd.	Bank of Africa Bank Ltd.	30.04.2004
EABS Bank Ltd.	Ecobank Kenya Ltd.	Ecobank Bank Ltd.	16.06.2008

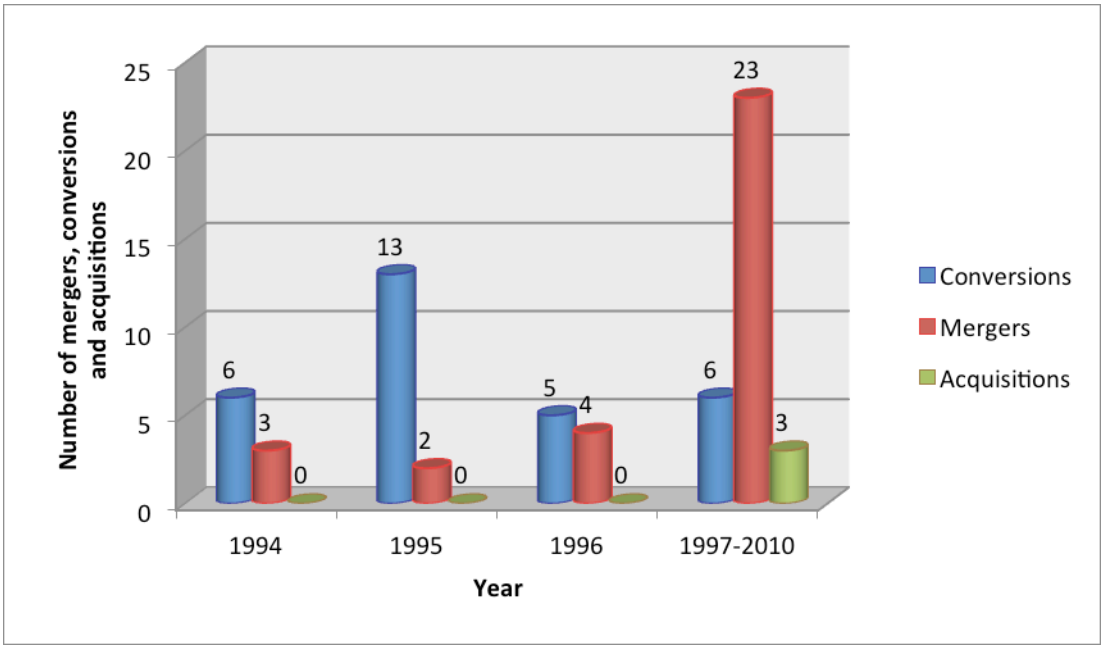
Summary of acquisitions in the Kenyan Banking Industry
(Source: Central Bank of Kenya, 2010)

II.F. Conversions in the Banking Sector, 1994-2007

No.	Financial institution (old name)	Commercial Bank (new name)	Date approved
1	Universal Finance Ltd.	Universal Bank Ltd.	03.11.1994
2	Akiba Loans & Finance Ltd.	Akiba Bank Ltd.	14.11.1994
3	Diamond Trust Company Ltd	Diamond Trust Bank Ltd	15.11.1994
4	Credit Kenya Finance Ltd	Credit Bank Ltd	30.11.1994
5	Consolidated Finance Ltd	African Banking Corp. Ltd	08.12.1994
6	Imperial Finance Co. Ltd	Imperial Bank Ltd	08.12.1994
7	Lake Credit Finance Ltd.	Reliance Bank Ltd.	13.01.1995
8	Habib Kenya Finance Ltd.	Habib African Bank Ltd.	26.01.1995
9	Finance Institution of Africa Ltd	FINA Bank Ltd	13.01.1995
10	Air Credit Finance Ltd.	Ari Bank Corporation Ltd.	07.03.1995
11	City Finance Ltd	City Finance Bank Ltd	23.03.1995
12	Credit Finance Corporation Ltd	CFC Bank Ltd	29.03.1995
13	Equatorial Finance Co. Ltd	Equatorial Commercial Bank Ltd	23.06.1995
14	Southern Credit Finance Ltd	Southern Credit Banking Corp. Ltd	26.09.1995
15	First National Finance Ltd.	First National Finance Bank Ltd.	19.04.1995
16	Prudential Finance Ltd.	Prudential Bank Ltd.	12.05.1995
17	Combined Finance Ltd.	Paramount Bank Ltd.	05.07.1995
18	National Industrial Credit Ltd	National Industrial Credit Bank Ltd	28.09.1995
19	Euro Finance Ltd.	Euro Bank Ltd.	20.12.1995
20	Victoria Finance Company Ltd	Victoria Commercial Bank Ltd	11.01.1996
21	Co-operative Finance Ltd.	Co-operative Merchant Bank Ltd.	27.03.1996
22	Investments & Mortgages Ltd	Investment & Mortgages Bank Ltd	27.03.1996
23	Credit & Commerce Finance Ltd.	Commerce Bank Ltd.	15.04.1996
24	Development Finance Co. Ltd	Development Bank of Kenya Ltd	20.09.1996
25	Charterhouse Finance Ltd	Charterhouse Bank Ltd	01.01.1998
26	Fidelity Finance Ltd	Fidelity Commercial Bank Ltd	07.03.1999
27	K-Rep Ltd	K-Rep Bank Ltd	24.03.1999
28	Equity Building Society	Equity Bank Ltd	28.12.2004
29	Akiba Bank Ltd	EABS Bank Ltd	31.10.2005
30	Family Finance Building Society	Family Bank Ltd	01.05.2007



Conversions within the Banking Industry
(Source: Adapted from Central Bank of Kenya, 2010b)



Overall activity of the Kenyan banking industry, 1994-2010
(Source: Adapted from Central Bank of Kenya, 2010 and 2010b)

Appendix III Research Instruments

III.A. Fraud Survey Questionnaire

1) Nature, trends and characteristics of fraud

This section assesses the industry's vulnerability to fraud. Please circle the number that represents your response.

1.1 How would you classify the problem of fraud in the banking industry?

1. Major problem 2. Minor problem 3. Not a problem

1.2 How would you assess the likelihood of frauds occurring in the financial sector over the next five years?

Very Likely	Quite Likely	Likely	Quite Unlikely	Very Unlikely
1	2	3	4	5

1.3 What in your opinion is the overall trend of fraud in the financial industry?

Increasing Rapidly	Increasing	Constant	Decreasing	Rapidly Decreasing
1	2	3	4	5

1.4 What do you think are the reason(s) for the trend in 1.3 above? Please circle a maximum of ***three*** of the most important reasons out of the possible reasons below.

1. Economic pressure
2. *More/less sophisticated criminals
3. Changing society values
4. Socio-cultural factors
5. Political factors
6. Effectiveness of justice systems
7. Advanced computer technologies
8. *Good/Poor ethical practices
9. *Good/Poor management practices
10. *Inadequate/Improved fraud training for those involved in fraud prevention
11. Other specify)_____
_____

(* delete as appropriate)

2) FRAUD EXPERIENCE

The degree of fraud varies from one organisation to another. In this section I would like you to think of a typical or the last fraud incident you can remember your organisation being involved in the last five years which resulted in a monetary loss.

Concerning the actual fraud tell us:

2.1 Who was/were the main perpetrator(s) of the fraud?

1. An internal perpetrator working alone
2. Collusion between internal perpetrators
3. An external perpetrator working alone
4. Collusion between external perpetrators
5. Colluding internal and external perpetrators

2.2 Who were the party/parties involved in the fraud? (Give at most the main 2 internal and 2 external parties)

Internal 1st Party

1. An Owner
2. An Executive (Director or Officer)
3. A Junior Manager
4. A Middle Manager
5. A Senior Manager
6. A Junior non-managerial employee
7. A Middle non-managerial employee
8. A Supervisor

Internal 2nd Party

1. An Owner
2. An Executive (Director or Officer)
3. A Junior Manager
4. A Middle Manager
5. A Senior Manager
6. A Junior non- managerial employee
7. A Middle non-managerial employee
8. A Supervisor

External 1st Party

1. A Customer
2. A Competitor
3. A Supplier
4. A Contractor
5. A Former Employee
6. An Organised Criminal
7. A Company Agent
8. Other _____

External 2nd Party

1. A Customer
2. A Competitor
3. A Supplier
4. A Contractor
5. A Former Employee
6. An Organised Criminal
7. A Company Agent
8. Other _____

2.3 What was/were the age(s) and gender(s) of the perpetrator(s)?

Party	***Age***	***Gender***
1. Internal 1st Party	1. Below 30 years 2. 31- 40 years 3. 41- 50 years 4. over 50 years	1. Male 2. Female
2. Internal 2nd Party	1. Below 30 years 2. 31- 40 years 3. 41- 50 years 4. over 50 years	1. Male 2. Female
3. External 1st Party	1. Below 30 years 2. 31- 40 years 3. 41- 50 years 4. over 50 years	1. Male 2. Female

4. External 2nd Party	1. Below 30 years 2. 31- 40 years 3. 41- 50 years 4. over 50 years	1. Male 2. Female

2.4 What type of fraud was it? (Circle any ***three*** at most)

1. Cash
2. Cheques
3. Credit card
4. Other negotiable instruments
5. Inventory (stock/supplies)
6. Kickbacks/bribery/corruption
7. Conflicts of interest
8. Identity
9. Fixed assets (Specify) _____
10. Other current assets (specify)_____
11. Intangible assets; specify whether
    a) Patents/copyrights/trademarks
    b) Confidential Information/Intelligence
    c) Goodwill
    d) Leasing
    e) Intellectual Property Rights _____
    f) Other Intangibles (specify) _____

2.5 What was the nature of the fraud? (Circle any ***three*** at most)

1. Theft
2. Diversion/Misappropriation
3. Conversion
4. Abuse/Misuse
5. Sabotage
6. Infringement
7. Other (specify)_____

2.6 What else did the fraud involve? (Circle any ***three*** at most)

1. Transfer of funds (e.g. wire transfer)
2. The use of computers
3. Identity fraud
4. Falsified accounts & financial statements
5. False invoicing
6. Fraudulent expense claim
7. Nothing else
8. Other (please explain)_____

2.7 What was (were) the perpetrators principle motivating factor(s) for committing the fraud? (Circle any ***three*** at most)

1. Gambling
2. Personal financial pressure (e.g. payment of school fees, debts etc.)

3. Greed
4. Lifestyle habits
5. Opportunity
6. Substance abuse (e.g. consumption to alcohol, drugs etc)
7. Corporate financial pressures (e.g. meeting corporate targets)
8. Other _____
9. Don't know

2.8 What was (were) the reason(s) given by the perpetrator(s) in justification of their fraudulent actions? (Circle at most any ***three*** responses)
1. Under-paid
2. Influenced/forced by others
3. Was just borrowing hoping to repay
4. Everyone else around them was fraudulent
5. Others are getting away with fraud and so they thought they also could
6. Was seeking revenge on the organisation for what they did to them
7. Had family pressure and taking the money was the only way to resolve it
8. Reasoned that the amount taken was not too large a sum
9. It was an opportunity to get rich quickly
10. Others (please explain) _____
11. Don't know

2.9 If possible, could you estimate the overall monetary loss from this fraud incidence as a percentage of business turn-over (income)?

1. Less than 1%
2. 1% - 5%
3. 6% - 10%
4. 11% - 15%
5. 16% - 20%
6. Over 20%
7. Don't know

2.10 Could you, if possible, quantify the direct loss to the organisation due to this fraud, either in value or as a percentage of business turn-over?

1. K.Shs._____ 2. _____ % 3. Do not know

2.11 Why did the fraud occur? (Circle up to any ***three*** reasons)
1. Poor screening procedures on hiring employees
2. Poor internal controls
3. Overrides of internal controls by management
4. Poor organisational culture
5. Lack of ethical culture (e.g. honesty, integrity etc)
6. Failure to punish offenders
7. Lack of fraud training

8. Poor inventory control
9. Poor record keeping and lack of adequate documentation
10. Use of new technology and systems
11. Other (specify) _____
12. Don't know

2.12 How was the fraud detected?

1. By accident/chance
2. Internal controls
3. External audit
4. Internal audit
5. Internal whistleblowers/fraud hotline
6. External whistleblowers (tip offs, complaints)
7. Third party investigations
8. Computer system controls
9. Anonymous letters/calls
10. Other (please specify) _____
11. Don't know

2.13 Who investigated the fraud? (Circle up to any ***three*** that apply)

1. Law enforcement body (e.g. Police)
2. Government regulatory body (e.g. KACC, CMA, Law Society of Kenya)
3. Internal investigation by Finance Department
4. Internal investigation by Security Department
5. Case reviewed by internal audit committee
6. External Auditors
7. Risk Manager
8. Forensic Accountants
9. Other (specify) _____

2.14 (a) What action(s) did the organisation take when this fraud was discovered?

	Internal Party		***External Party***	
	1st	2nd	1st	2nd
1. Immediate dismissal	[ ]	[ ]		
2. Disciplinary action other than dismissal	[ ]	[ ]		
3. Allowed employee(s) to resign	[ ]	[ ]		
4. Civil prosecution for recovery	[ ]	[ ]	[ ]	[ ]
5. Criminal prosecution	[ ]	[ ]	[ ]	[ ]
6. Negotiated settlement	[ ]	[ ]	[ ]	[ ]
7. Took no action	[ ]	[ ]	[ ]	[ ]
8. Other action (please specify) _____	[ ]	[ ]	[ ]	[ ]

(b) In case of criminal or civil prosecution what was (were) the outcomes?

	Internal Party		***External Party***	
	1st	2nd	1st	2nd
1. Acquittal	[ ]	[ ]	[ ]	[ ]
2. Conviction	[ ]	[ ]	[ ]	[ ]
3. Negotiated settlement	[ ]	[ ]	[ ]	[ ]
4. On-going case	[ ]	[ ]	[ ]	[ ]

(c) What was the extent of financial recovery?

	Internal Party		***External Party***	
	1st	2nd	1st	2nd
1. 0%	[ ]	[ ]	[ ]	[ ]
2. Partial (give % of recovery)	[ ]%	[ ]%	[ ] %	[ ]%
3. Full (100%)	[ ]	[ ]	[ ]	[ ]

3. FRAUD PREVENTION

In this section I would like to find out how your organisation carries out fraud management, the counter-fraud measures being employed and the costs of fraud.

3.1 What measures have/are being taken to prevent fraud in your organisation? Please rank up to ***five*** of the most important ones with '1' = the most important, '2' = the next most important to '5' = the 5th most important

Circle	Measure	Rank (1-5)
1	Improvement or review of internal controls	
2	Establishing fraud prevention policies	
3	Establishing an ethical code of conduct	
4	Implementing a fraud hotline (whistle blowing)	
5	Training employees on fraud prevention and detection	
6	Screening/reference checks on new employees	
7	Establishing a fraud budget	
8	Automated fraud prevention e.g. use of surveillance equipment (cameras)	
9	Staff rotation policy	
10	Security department	
11	Ethics training	
12	Use of forensic accountants	
13	Close supervision	
14	Fraud auditing	
15	Inventory observation	
16	Surveillance of electronic correspondence	
17	Limiting opportunities	
18	High deterrence measures	
19	Spot checking	
20	Asset Protection programs	

21	Other (specify)	

3.2 Please indicate what fraud technology/software you use, stating whether it is internally or externally developed and the perceived effectiveness of the application

Fraud software	(Circle as appropriate)	Tick Internally or externally developed Int. = Internally Ext. = Externally	Effectiveness 1 = Very effective 2 = Effective 3 = Ineffective 4 = Not sure
1. Filtering software	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
2. Firewalls	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
3. Password protection	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
4. Continuous auditing	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
5. Discovery sampling	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
6. Virus protection	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
7. Financial ratios	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
8. Digital analysis	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
9. Data mining	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
10. Other (specify)	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4
11. Other (specify)	Yes [ ] No [ ]	Int. [ ] Ext. [ ]	1 2 3 4

3.3 How much fraud do you think your organisation detects on an annual basis? (Insert estimated percentage either by value and/or by number of incidences)

By Value (K.Shs) _____ % of the total value of fraud is detected

By No. of incidences _____ % of number of fraud cases are detected

3.4 How often do fraud prevention methods get reviewed?

1. Quarterly
2. Half yearly
3. Annually
4. Less frequently
5. Continually
6. After a fraud incidence
7. Other (specify) _____
8. Don't know

3.5 Who is responsible for carrying out the review?

1. C.E.O
2. Accountant
3. Internal Audit committee
4. External Auditors
5. Other (specify) _____
6. Don't know

3.6 Can you quantify how much of the organisations annual turnover you think has been lost to fraud in the last financial year?

_____ %

4) PERSONAL AND ORGANISATIONAL INFORMATION

4.1 Which of the following best describes the operations of your institution? (Circle as appropriate)

1. Local Bank
2. National Bank
3. National subsidiary
4. International Bank
5. International Subsidiary
6. Other (specify) _____

4.2 What type of entity is your organisation?

1. Public Limited Company
2. Private Limited Company
3. Public Sector (Government)
4. Other (specify) _____

4.3 How large is whole organisation based on number of employees? (Tick as appropriate)

[ ] 0-100 [ ] 101-500 [ ] 501-1,000 [ ] 1,001-10,000 [ ] Over 10,000

4.4 What role do you perform in the organisation?

_____

4.5 How many years of experience do you possess?

Years of overall accounting/auditing experience	
Years worked in present banking institution	

Thank you for taking your time to participate in this survey!!!

Kindly return the completed questionnaire using the freepost self-addressed envelope provided.

III.B Interview Schedule

1) How large is the audit/ fraud/security department? (no. of employees)

2) How important are your external auditors in fraud detection? Why?

3) Please nominate the type, value and perpetrator of the **largest single fraud** you can recall in the past five years

Type of fraud	
Perpetrators	
Factors contributing to the fraud	
How was the fraud detected	
How much of the funds were recovered	
Was the matter reported to police	
How much did it cost to investigate the fraud	
What was the total loss incurred?	

4) Where fraud involved internal perpetrators could you provide details about the perpetrators

Gender	
Age	
Position in employment	
Length of service within organisation prior to the fraud occurring	
Duration of service in current position at time of committing the fraud	
Motivation for the fraud	
Period of time elapsed before fraud was discovered	
Did internal perpetrator have a known history of dishonest conduct	
Did the person act alone, with internal or/and external collusion	
Did the perpetrator have a history of fraud? What type of prior fraud(s) had the perpetrator committed?	
What action was taken against the perpetrator (s)?	
Was the action an adequate deterrent?	

5) What did you learn from this incidence?

6) Has the incidence helped the organisation improve its' fraud prevention and detection methods?
7) What can be done to prevent this type of fraud occurring again?
8) Do the banks share about their fraud experiences at industry level?
9) What measures are banks putting in place jointly to reduce the incidence of fraud?
10) Has the organisation had any fraud incident involving the misuse of computers/computer networks/online banking or organised criminal groups?
11) Has internet banking increased your banks vulnerability to fraud?
12) How has the bank protected itself by the use of fraud software and technology?
13) Does the organisation have a budget for fraud?
14) How much is the fraud budget as a percentage of the total budget?
15) Has this budget increased over the past five years?
16) Are all employees educated on anti-fraud measures and policies?
17) How are anti-fraud policies communicated to employees
18) Are employees provided with training on how to implement the fraud policies?
19) Which anti-fraud measures have been most effective in combating fraud? How?
20) Does your bank have a code of ethics and are all the employees aware of it?
21) Has the organisation experienced any unethical behaviour in the past 5 years?
22) Who is responsible for developing an ethical culture in the organisation?
23) What type of unethical behaviour has the organisation experienced on a regular basis in the past 5 years?
24) What cultural and factors contribute to unethical behaviour in your organisation?
25) Are you aware of certain types of frauds, existing in other countries, that could likely find their way into the Kenyan Financial Sector?
26) What measures are being put in place to combat such emerging frauds before they hit the industry?
27) What can be done to reduce fraud in the banking industry in Kenya?
28) How do you enforce deterrence in a positive way?
29) In the process of fraud there are four main elements, namely: Prevention, detection, investigation and prosecution. Could you briefly discuss some of the challenges the organisation faces in these areas?

    Prevention –

    Detection –

    Investigations –

    Prosecution –

30) General Comments

Appendix IV Sample Interview Outcomes

INTERVIEW - ADAM (Participant No. 005) – National bank

1) How large is the audit department (no. of employees)
The audit department consists of 4 people. We also have a compliance department and it consists of 2 people.
2) How important are your external auditors in fraud detection? Why?
Hmm..mm …. to some extent not so much really with external auditors because basically they depend on internal audits. The reports that they review are mainly done by internal auditors. They will possibly do some recommendations but they never get to the ground. Basically what they are looking for is potential loss to the institution for financial purposes….and that is really what they do
3) Please nominate the type, value and perpetrator of the **largest single fraud** you can recall in the past five years

Type of fraud	*We have many frauds happening almost on a daily basis, just to mention - cheque issuance. Fraudulent cheques are passed on and are normally paid on the wrong accounts. On the compliance side there is a deterrence called Know Your Customer (KYC). However, we still find that cheques are intercepted through clearing or they are substituted with fake cheques. By the time you get the cheque, the cheque will be fraudulent, the good cheque would have gone elsewhere and the funds are gone. We have quite a number of these cases happening everyday. I will just mention about a case of a transfer which involved a cheque. This case happened offshore. We received a foreign cheque drawn on an overseas bank (a German Bank) and the cheque was drawn in Euros. As usual we don't give immediate credit we normally send these cheques on collection basis to the paying bank, which we did. We got the credit later, an indicator that the cheque had been cleared offshore. We then proceeded to avail the funds to the payee. Three months later we got information*

	from Germany saying that the cheque we had paid was unpaid! We were informed that the cheque had been fraudulently obtained through a robbery in one of the countries but had filtered into Kenya, where someone was dishing out the cheques for payment of various facilities. In view of their laws in Germany we had no option but to take the hit. We got hold of the payee, who happened to be one of our customers' customer and the case is still pending in court. It has taken us the last three years or so.
Perpetrators	*A customers' customer. The perpetrator was paying for goods supplied by one of our customers, banking the same fraudulent cheque into the customers account. The customer was deemed to have received good funds. So the loss fell on the bank. There was no deposit clause for recourse to state what would happen if the cheque returned unpaid after funds had been availed. Today we on our deposits we have a clause for recourse such that in case the cheque returns unpaid the individuals account is debited*
Factors contributing to the fraud	*The fact that the fraud occurred outside the country made it difficult to for us to monitor it. Infact, the perpetrator had claimed to be an NGO in Uganda and he had been given a cheque as an NGO because he was setting up an office in Kenya! Apparently when the cheque was returned unpaid we were told that the office of the German Embassy in Uganda had been broken into in an incidence of robbery with violence (resulting in the death of a guard). The proceeds of the cheque were being used to purchase furniture and furnishings for the new office that was to be located in Kenya – which never happened to be. The German police came in to testify. Unfortunately there were fears of threats to the witnesses from Germany (as per Interpol). But finally they did come in and*

	testified. The original cheque was retained by the police in Germany for investigations and we are yet to hear from them as of date. So the case is still held up.
How was the fraud detected	*The case of the stolen cheques had already been reported to the German police, but the paying bank was not aware. It is only in the process of the investigation that they realised one of the cheques had come through.*
How much of the funds were recovered	*Shs. 8 million – some of the goods purchased with the fraudulent funds were traced, recovered and sold through a court action*
Was the matter reported to police	*Yes*
How much did it cost to investigate the fraud	*We have no cost on our side other than time taken up going to court and the Shs. 3 million losses. The police are the ones who are investigating the fraud. We wrote off the fraudulent cheque amount within the year it occurred. If we ever get the money back we will write it back!*
What was the total loss incurred?	*The loss was 11 million Shillings. But the net loss was eventually 3 million. We have an insurance cover but in this case there was no insurance recovery as the fraud occurred outside Kenya.*

4) Where fraud involved internal perpetrators could you provide details about the perpetrators?

Gender	*Male*
Age	*In mid 40's*
Position in employment	
Length of service within organization prior to the fraud occurring	
Duration of service in current position at time of committing the fraud	
Motivation for the fraud	*The fact that he was associated with or dealing with a group of politicians (peer pressure) and he perhaps wanted to remain in their good books*
Period of time elapsed before fraud was discovered	*3 months*
Did internal perpetrator have a known	

history of dishonest conduct	
Did the person act alone, with internal or/and external collusion	*Alone*
Did the perpetrator have a history of fraud? What type of prior fraud(s) had the perpetrator committed?	*Yes. We discovered that he had been involved in other fraudulent transactions (with part of the same series of fraudulently stolen cheques) with other local banks (Standard bank & National Bank) and a South African group. He had purchased furniture from a company called Supreme (from South Africa) and paid with one of the fraudulent cheques. At that time, the other local banks did not co-operate with our enquiries on this person and on those orders…they said they had nothing. It was only six months later they came crying saying "yes, we should have heard from you!" They were also hit and also suffered a loss because their cheques were also returned unpaid and it took them longer to recover their money.*
What action was taken against the perpetrator (s)?	*He was arrested and prosecuted*
Was the action an adequate deterrent?	*For foreign cheques we are bound by offshore regulations which are drawn according to the rules and regulations in other countries. So in Kenya if a cheque is 6 months old it is stale and cannot be drawn. But offshore they have regulations, in the USA of UK and the instruments can be drawn even after 1 year and for correspondent banks could take for as long as they wish! So internationally am not sure if it is an adequate deterrent.* *However, locally, I can say that arresting a person and taking them to court is indeed a good deterrent. Because once you do that someone will start thinking twice unless he is a criminal…but no is born a criminal anyway, that is the much we know…but people just turn to one because of greed*

	Interviewer: Is he currently in prison or is he on bail. *Interviewee: This is the other ironic part of it! I got him arrested in my office. When he was arrested he was taken to the police station and was locked in. I appreciate the way the police moved swiftly on that day of the arrest making it possible for us to retrieve all the goods - the furniture, bicycles, electronics, cameras, videos cameras that he had bought from this coming….because they moved the same night and picked all these things from the Western side where this person (politician) came from. Interestingly after the arrest the perpetrator was in custody for 3 months and was released on bail. After that the guy did not care any more. When he reports to court he comes with friends whom he says are his colleagues in the NGO. Him and the politician (our customer) do not seem interested or concerned about the case which has really dragged on with various reasons being given by the perpetrator and his lawyers for not having the case heard before the court. The guy is still running free* *Interviewer: Does that make you frustrated?* *Interviewee: Yah, actually you feel frustrated because you have got all the facts and you go to court….again I am talking about the judiciary…. You go there you are in there day in day out, for a year two years…you sometimes loose taste of it. Most of us have testified except our customer, who also doesn't seem to be keen because he is not at a loss. He doesn't seem to take a keen interest because every time they are bonded there is always an excuse. Initially we used to have the excuse with the lawyers of the culprit, the fraudsters lawyers… they*

	would never turn up in court, or it would be said he is in another court or he is sick….or this…until eventually the magistrate ruled that the case would proceed with or without lawyers.

[Points of interest: The perpetrator was associated to some political leader (a former MP) and this was around the election campaign period in 2005. Towards the election is when these things happened. So apparently this money was being used for the 2007 election campaign. One of the consignments had 60 bicycles – "Bodaboda" which was going to be dished for election purposes. When this person came he portrayed himself as a Professor/Lecturer at the Makerere University in Uganda. As he was introduced to the bank by the politician who was a customer we opened an account for him. He used to come every Monday morning and you will only see him in Nairobi and you will not see him until a week later as he claimed to be busy and could only come over the weekend.]

5) What did you learn from this incidence?
When you get a customer introduced to you, you must ensure that you find out more about the person. Because we did not know this person, we knew our customer who had banked a cheque in his account. But you see we eventually opened an account for him (fraudster) through our customer… but we didn't know much about this customer. We learnt that we must know our customer and where to find them. Due diligence must be taken before we open an account. Customers must give something like a utility bill as proof of where you live or operate from (in case of a business). We also now carry out prompt or abrupt visits to the address given by a customer. Every three months we visit business premises to avoid problems associated with 'brief case' businesses.

6) Has the incidence helped the organization improve its' fraud prevention and detection methods?
Yes, we have improved our controls on account opening.

7) What can be done to prevent this type of fraud occurring again?
Just KYC

8) Do the banks share about their fraud experiences at industry level?
Yes. Under the Kenya Bankers Association we have a Fraud and Securities Committee that meets every three months (or as and when is necessary when an urgent matter arises). The committee has representatives from all banks and I happen to be a member of the committee. In the past banks used to be so rigid in trying to keep things to themselves…I don't want you to know…I don't want this bank to know what we are going through. But now it is an industry norm that if this person hits one bank today, tomorrow it will be another bank. Apparently the perpetrator we are talking about had committed a similar crime in Standard Bank and another one in the

National Bank. So we realised had we shared the information this person would not have succeeded in opening an account.

9) What measures are banks putting in place jointly to reduce the incidence of fraud?

We have set up a database that acts like a reference bureau where banks can make reference to individuals who are blacklisted. We share information now openly. We also use the forum to criticise those who are not observing the KYC rule and paying attention to internal controls. We all want business, so you find banks are bending rules here and there, but we encourage each other not to do so. One of the key things we think will be a good deterrent in the industry is to have the paying bank confirm that the cheque is good. So the cheque is cleared by the paying bank first. If the cheque turns round to be fraudulent then the paying bank ends up being at a loss. However, the collecting bank must also be responsible and know the person you are giving the money. If this recourse is in place then both the paying and collecting bank are alert and seek to know their customer as the recourse would make them liable to repay the money within the period of one month. This would be a major deterrent when it will become effective.

Unfortunately we have fake documents readily available to the public which fraudulent individuals can use to carry out identity fraud. When you walk around on some our streets you can get an ID. Or there is impersonation; somebody picks up your ID goes put his photo in it puts their picture in your Id and transacts with it…it is happening.

10) Has the organization had any fraud incident involving the misuse of computers/computer networks/online banking or organized criminal groups?

We have been reluctant to enter into internet banking but that is where the industry is moving and we cannot avoid going in the same direction. Very recently we launched an online service for our customers. Customers are given their internet profile and they have a password that is intended to protect them and provide privacy and security online. However, we have network hackers who get into the system, pick up information and do whatever they want.

Interviewer: Any problem with organized criminal groups?
Interviewee: No we have not had problems with organized criminal groups. We haven't seen much of that. The only thing is that they may be organized…because what we have realised there are some people do absolutely nothing other than but to sit in some of the cafes in this country….they operate from cafes I tell you…and that is where they transact from. Maybe they are waiting for a cheque! Let's assume there is an internal fraud facilitated by someone internally… he might take your signature for the person (fraudster) to practise and on so he can sign the cheque and pass it through

12) Has internet banking increased your banks vulnerability to fraud?

For sure it has….We have not had any internet fraud activities. But we are definitely now more vulnerable to fraud. For example, we developed a certain product (NIC MOVE) which really hit the market and everyone now knew of our banks presence. That is the time we started getting the highest number of fraudulent cheque frauds. Some individuals opened up accounts with fake documents and contact details – and you will think this a company and these are their directors. We used to do a call back. But unfortunately the number reflected on the letter heads would be the number of the same fraudsters.

13) How has the bank protected itself by the use of fraud software and technology?
The challenge of trying to keep hackers off and arrest them is a difficult one. As a measure we have put up firewalls that you will be able to go to a certain level and you can't proceed further. We have six months testing that you can't access our systems or break in. The firewalls have different levels of access requiring different passwords. It increases the degree of difficulty in trying to access the system. We look at day to day transactions on the system to identify any anomalies through an audit.

14) Does the organization have a budget for fraud?
No, because it is not something we think would happen and it would happen once in a while. We have not really had significant levels of fraud to warrant a separate, distinct budget. The case I talked to you about was the one major case we have ever had. Most of the cases that occur occasionally involve small sums of money.
15) How much is the fraud budget as a percentage of the total budget?
16) Has this budget increased over the past five years?
17) Are all employees educated on anti-fraud measures and policies?
We have a fraud policy which also includes the red-flags and I carry out training every six months for all staff. If there are new members of staff we also take them through the fraud policies.
18) How are anti-fraud policies communicated to employees
Our policy is on the company website and staffs are expected to read it. We also have handy folders that every staff member has and one can make reference to it.
19) Are employees provided with training on how to implement the fraud policies?
Yes, we carry out internal training. Personnel whose jobs directly relate to fraud prevention are taken to external courses (workshops and seminars)organized by the Central Bank, the Kenya Bankers Association and other private organizations. During the training case studies are given out so that the employees can relate with real life stories and issues in fraud. Such case studies are used to train the employees on detection of fraud and implementation of the policies.

20) Which anti-fraud measures have been most effective in combating fraud? How?
Training has been effective as well as internal audit. We also have call backs to payees when big cheques are presented to the bank. However, with time fraudsters come to learn what the limit requiring call backs is and they bring cheques that are below the callable level.

21) Does your bank have a code of ethics and are all the employees aware of it?
Yes, we have a code of ethics and every employee must sign the code. Every 6 months the HR department issues a form to all employees who are required to attest that they have re-read the code of ethics and sign.

22) Has the organization experienced any unethical behaviour in the past 5 years?
Yes, I have had two separate cases where staffs have taken money from customers with the intention of putting it into the customers account and it never happened. In one of the case the customer was repaying a loan and the loan became overdue. The customer when faced with repossession of their assets enquired and insisted that he had been paying in the money.. In the course of investigating it was found that the staff member had taken the money. The employee was dismissed. In the other case, a staff member took some money from a client in the pretext of writing down accrued charges on commission. All these incidences occurred 4 years ago and led to the code of ethics being signed continuously rather than just upon entry as in the past

23) Who is responsible for developing an ethical culture in the organization?
Director of Human Resources and all other Managers contribute to the ethical culture. New employees undergo a two weeks induction and it is then that they are made aware of the code of ethics and the all the policies. The employee is expected to familiarize themselves with all these.

24) What type of unethical behaviour has the organization experienced on a regular basis in the past 5 years?
25) What cultural factors contribute to unethical behaviour in your organization?
No, there are no specific cultural issues that I can point out, but there are social factors that show up due to peer competition and pressure. You will find that there is an age group (20-30's) that is particularly involved in fraud

26) What do you perceive to be the implications of unethical behaviour on your business?
27) Are you aware of certain types of frauds, existing in other countries, which could likely find their way into the Kenyan Financial Sector?

Not really, because some of the more recent frauds like card fraud have reached Kenya. There were people with what we call "White cards" withdrawing a lot of money from ATMS' here but apparently the clients are offshore. One of them used our ATM & was arrested. There was no complainant locally as the accounts were off-shore accounts. So the guy has ended up free.

28) What measures are being put in place to combat such emerging frauds before they hit the industry?
Kenya Bankers is assisting in developing fraud prevention measures that the industry can use. We can already see the effectiveness of the measure by the fall

in number of bank robberies. This is due to measures being given out to banks through the Kenya Bankers Association

29) What can be done to reduce fraud in the banking industry in Kenya?

30) What kind of compliance techniques do you use to ensure that fraud losses are minimized?

We use limits and call backs to also check that there is compliance with bank rules. We have maker – checker distinctions.

31) How do you monitor effectiveness and success of your security and fraud control measures?

We look at the number of incidences that have occurred on a monthly basis to capture the trends in the numbers, nature and types of frauds

32) How do you enforce deterrence in a positive way?

The staff members first of all are well paid to encourage them not to get involved in fraud. We encourage anonymous whistle blowing and give monetary rewards to staff who help in preventing an attempted fraud or who give vital information that leads to the frustration of a fraud. Sometimes people come forward openly and say what is happening. If it happens to be true then they are rewarded.

33) In the process of fraud there are four main elements, namely: Prevention, detection, investigation and prosecution. Could be briefly discuss some of the challenges the organization faces in these areas?

Prevention – There is a problem with getting co-operation when looking for necessary and vital information that can help to prevent the occurrence of a fraud.

Detection – Retrieving the documents that you need for evidence. Fortunately we have different people with different responsibilities. The person who keeps the cheques is different from the person who did the processing. Now unfortunately…so when you approach say the person who handles cheques and ask for a specific cheque, they assume you are following up a fraud, which may not be the case; I may want to see it for a different reason. Management support is essential in getting documentation

Investigations – Mostly the crime is committed from elsewhere and it only filters to you as the paying bank. It is hard to investigate frauds (collusions or external) directly

without having to involve the police, Central Bank or the Court. It is a big drawback. Even other banks that are players in the industry are not very co-operative when it comes to investigation. Unless we agree … because there is a crime that has been committed over that account can you freeze that account or block that account until we settle this matter…that does not happen! Most of the cases will tend to be cheque frauds and it drags forever.

Prosecution – Cases drag on for a very long time. Cases are just mentioned and you are told to wait for another date and that date is not tomorrow. The earliest I have seen is duration of 3 months. Especially when it comes to September – October you will not get a hearing in the current year because you will be told the diary is full.
The other element of it is that you are dealing with a criminal and you do not know what this person is going to say about you out there in the streets. There is the threat to physical security (in that you can end up becoming a victim of the fraudster).

33) General comments

KYC is very important in fraud reduction and prevention for the industry. If we move liability to the collecting bank as opposed to the paying bank then there will be more diligence on part of the banks. As you receive a deposit into your customers account, you must know this customer is well known to me and if I was to produce them I would be able to. If there is fraud committed over this that account I will be able to get this person. But you will find because we all want money, we are rushing to win any type of account…we don't even care about the documents, because at the end of the day we are looking at the bottom line – what are your profits at the end of the year, hoping all is going to be well!

The other thing is the market place, the environment we are living in! We have so many of unemployed people. When they sit down they don't think of anything positive other than how they can get money and how they can mug you. When they mug you they take your cheque book and tomorrow your cheque book is already withdrawing money in your account. These are the things that are in the society and if we can get these ones out, I think we will be in the right direction.

Appendix V – List of Interviewees

Participant No.	Pseudo (Code) Name	Type of Bank
001	Gabriel	Regional
002	Ruth	Regional
003	Moses	International
004	Joseph	Local
005	Adam	National
006	Joel	Regional
007	Joshua	International
008	Caleb	Local
009	Titus	National
010	Solomon	Local
011	David	Regional
012	Elijah	International
013	Jacob	Local
014	Abraham	International
015	Thomas	Regional
016	Simon	International
017	Paul	Local