STRATEGIES ADOPTED BY COMMERCIAL BANKS IN KENYA TO COMBAT FRAUD: A SURVEY OF SELECTED COMMERCIAL BANKS IN KENYA

Jimmy Mutuku Mwithi
Kenya Methodist University

Dr. Joseph Ngugi Kamau
Lecturer, Kenya Methodist University

ABSTRACT

Over the past 10 years, commercial banks across the globe have experienced an upsurge of losses arising from frauds that affect customers’ accounts as well as the banks’ internal accounts. In Kenya, as in other rapidly developing countries, the impact of the upsurge in frauds has been particularly hard on the fragile financial infrastructure. The discussions of this paper sought to explore strategies adopted by commercial banks to combat fraud in commercial banking sector in Kenya. Specifically the paper sought to explore influence of know your customer, crime and anti-money laundering, technology and internal controls issues to combating fraud. Based on the objectives, the study concluded that legal Framework set by organizations and central banks such as verification of client personal information assist in combating fraud to a great extent. Most of the organization had access to personal and private information that they use in combating fraud to a great extent. On internal control, the study concluded that commercial banks are major institutions responsible for controlling accounts conducts and relationship. Finally, the study concluded that Real Time Gross Settlement (RTGS) mode of payment is associated with less frauds compared to manual methods of payments to a great extent.

Key Words: Customer, Technology, Control, Laundering, Fraud and Strategies

INTRODUCTION

Over the last one decade, commercial banks have seen a sharp increase in the number and value of frauds, much to their distress. However 2009-2011 has seen a steep upsurge in incidences of fraud. The main cause of the unprecedented upsurge can be attributed to staff complicity and collusion with third parties (Adams & Sasse, 1999). The technological advancement being embraced by the industry poses a risk as system vulnerability is taken advantage of by fraudsters who gain insight of the weaknesses through collusion with dissident staff members (Beck et al, 2007). The following are the common fraud typologies being experienced in the industry: Frauds through staff complicity and collusion, Frauds through Electronic Funds Transfer, IT frauds, Identity fraud, Forgery, Cheque frauds, Card Fraud, Clearing frauds (KRA frauds), Fraudulent letters of instructions, Recruitment fraud, False claims by staff, Procurement fraud, Advance fee fraud, Diversion of commissions, Cash suppression.

According to Wambugu (2008) the banking sector has, in the recent years come under increasing threat of operational risks, which affects their performance. These operational risks mainly arise from the ever-increasing incidents of fraud, which in one way or the other involve banking staff. For instance, between 2009 and 2010 July banking institutions lost KShs 2.4 billion through a criminal syndicate using the latest technology.
Frauds bedeviling banking industry are generally not new. Even though various measures have been taken to minimize the incidence of fraud, its incidence is still on the rise by the day because fraudsters have continued to device tactical ways of committing fraud. This has become a point of great concern in the banking sector and by extension as well as every business organization in Kenya. Although this phenomenon is not unique to the banking industry or peculiar to Kenya alone, the high incidence of fraud within the banking industry has become a problem to which solution must be provided in view of the large sums of money involved and its adverse implications on the economy (Adeduro, 1998).

This research project is centered on strategies adopted by commercial banks in Kenya to combat fraud and it has focused on selected commercial banks in Kenya. The study was taken against the backdrop that the banking sectors is a key pillar to the achievement of vision 2030.importance of Kenya’s long term development agenda spelt out in the vision 2030, targets an annual growth rate of 10% in the medium term with an investment rate of 30% of which a significant proportion will be financed through mobilizing domestic savings through financial sector which is viewed as substantially diversified and is dominated by banking institutions which have not evolved to provide long term capital adequately ((Ngugi & Njenga, 2008).

**PROBLEM STATEMENT**

According to a report by Delloite (2012) East African banks lost Sh4.05 billion ($48.3 million) to fraud in the 18 months ended June this year, mainly through insider collusion. The amount is equivalent to a full year profit for small or medium-sized banks in Kenya. According to the report, crime statistics by the one of the East African countries police force indicates a 14 per cent increase in economic crimes from 2,662 reported cases in 2010 to 3,036 in 2012. Out of all reported cases, it is electronic money transfer methods that pose the greatest risk to commercial banks in East Africa. Statistics from a recent Central Bank of Kenya’s supervision show commercial banks are losing an average of Sh100 million to fraudsters every month. Banking fraud experts say the figure is varied, depending on the level of exposure of the financial institutions (Gaitho, 2003). Those with the highest number of branches or most tech-savvy are worst affected by the trend. Recent CBK data on fraud also showed incidences of banking fraud have risen by between three to five per cent of total financial transactions, from as low as 0.5 per cent, in the last five years (CBK, 2009). According to Banking Fraud Investigation Unit (2011) during the 1st quarter of year 2011, cheque fraud was the most common type of fraud while in the 2nd quarter forgery was leading. Same was the case in the 3rd quarter. Forgery rose mainly after cheques were stolen and signatures were forged. There were also cases where deposit slips were forged and fraudulent instructions issued to make transactions. According to data from the Banking Fraud Investigations Department (BFID), financial institutions reported Ksh1.49 billion ($17.52 million) stolen from customers’ accounts between April 2012 and April 2013.
Investigators managed to recover only Ksh530 million ($6.2 million) and at least Ksh1.5 billion ($17.64 million) from Kenyan banks in the past one year, in schemes hatched by technology-savvy bank employees. The data indicates that between November 2012 and April this year alone, a total of Ksh952 million ($11.2 million) was stolen. Of this, only Ksh345 million ($4.05 million) was recovered. Growing cases of fraud and cyber crime mean that financial institutions need to urgently invest in detection and preventive mechanisms as today's fraudsters are increasingly sophisticated. The incidents of fraud have continued to take the lead owing to the advancements in technology. The expansion of modern technology has resulted in the facilitation of daily activities, but rendered lives more vulnerable to fraud attacks. Thus the banking sector among other institutions should not down their tools in an effort to curb the rising incidences of fraud; therefore this study analyzes possible control strategies adopted by commercial banks, and other Financial Services Companies in Kenya to combat fraud-related challenges.

**GENERAL OBJECTIVE**

The main aim of this study was to analyze strategies adopted by Kenyan commercial banks to combat fraud with specific focus to selected commercial banks in Kenya.

**SPECIFIC OBJECTIVES**

1. To investigate the role of Crime and Anti-Money Laundering (AML) Act in preventing fraud in commercial banks
2. To evaluate the concept of Know Your Customer (KYC) and its impact in preventing fraud among commercial banks.
3. To evaluate the impact of technology in preventing fraud in commercial banks
4. To determine the effects of internal controls in preventing fraud in commercial banks

**LITERATURE REVIEW**

This is a collection of interrelated ideas based on theories. This study will be guided by the following theories:

**Classical Criminology**

Classical criminology grows out of a reaction against the barbaric system of law, justice and punishment. It seeks an emphasis on free will and human rationality. The Classical School was not interested in studying criminals, but rather law-making and legal processing. Crime is
activity engaged in out of total free will and that individuals weigh the consequences of their actions. Punishment is made in order to deter people from committing crime and it should be greater than the pleasure of criminal gains. Classical theory emphasizes a legal definition of crime rather than what defined criminal behavior. Crime occurs when the benefits outweigh the costs when people pursue self-interest in the absence of effective punishments. Crime is a free-willed choice (Kohlberg, 1976).

**Theory of Anomie**

Anomie refers to a breakdown of social norms and it a condition where norms no longer control the activities of members in society. Individuals cannot find their place in society without clear rules to help guide them. Changing conditions as well as adjustment of life leads to dissatisfaction, conflict, and deviance. He observed that social periods of disruption (economic depression, for instance) brought about greater anomie and higher rates of crime, suicide, and deviance (Cohen & Felson, 1979).

**Routine Activities Theory**

Routine Activities states that criminal offenses are related to the nature of everyday patterns of social interaction. Cohen and Felson, (1979) used their approach to explain the rise in crime between the years 1960 to 1980 in USA. They were concerned with the changes occurring in society, which they believed led to social disorganization, which further led to crime opportunity. Their perspective shows that crime is not solely related to biological and psychological characteristics, or to social or economic conditions, but that it is just as important to concentrate on situational factors which give rise to criminal opportunity. Routine activities approach is important to crime prevention and to the changing of conditions and circumstances in which crime is committed.

**Cognitive Theory**

According to this approach, criminal behavior results from the way in which people organize their thoughts about morality and the law. Kohlberg (1976) a developmental psychologist, formulated a theory concerning the development of moral reasoning. He posited that there are three levels of moral reasoning, each consisting of two stages. During middle childhood, children are at the first level of moral development. At this level, the pre-conventional level, moral reasoning is based on obedience and avoiding punishment. The second level, the conventional level of moral development, is reached at the end of middle childhood. The moral reasoning of individuals at this level is based on the expectations that their family and significant others have
for them. Kohlberg found that the transition to the third level, the post conventional level of moral development, usually occurs during early adulthood. At this level, individuals are able to go beyond social conventions. They value the laws of the social system; however, they are open to acting as agents of change to improve the existing law and order. People who do not progress through the stages may become arrested in their moral development, and consequently become delinquents.

**Concept of Fraud**

Fraud is a human activity which is mostly attributed to the following: inadequate or lapses in control i.e. lack of adherence to the laid down procedures/guidelines by staff, negligence by members of staff, inadequate supervision, or the absence of control procedures in the bank. Inadequate training and or knowledge by members of staff i.e. staff not knowing the correct procedures, inadequate knowledge of the banks products (Sartre, 1981). Double standards in Management practices, dishonesty by members of staff, collusion between staff and customers or members of the public or between staff themselves, rapid changes which have taken place particularly the computerization of processes, inadequate staff hiring practices which do not ensure sufficient vetting of prospective candidates, lack of compliance with essential work ethics, over-riding controls by managers, inadequate auditing, over concentration of duties in the hands of one person (Lack of segregation of duties), and over dependence on one member of staff on particular processes. It is recognized that for the Bank to fight fraud effectively, we must understand fully the causes of fraud and in what particular areas within the Bank fraud occurs (Sartre, 1981).

Fraud is believed to be amongst the most serious corporate problems, and challenges in today's business environment, indeed Palshikar (2002) suggests that fraud or scam is a dominant white collar crime in today's business environment many businesses and government organizations, particularly in financial and related services, suffer from fraud of various kinds. In the banking industry, many frauds are perpetrated through falsified payment instruments. Common fraud types include; Cheque fraud, computer fraud, Card fraud and Mail order fraud that’s commonly referred to as internet fraud. Fraud has the effect of reducing the assets and increasing the liability of any company. In the case of banks, this may result in the loss of potential customers or crisis of confidence of banking public and in the long run end up in another failed bank situation. It is instructive to know that many banking operatives have different reasons for joining various banks. Many have the intention of working for a short time in the banking industry (get whatever they can and find another job that is less demanding); some are in the industry because of their love for banking and all it stands for. A majority are there to enrich themselves by fraudulent means. Due to the upsurge of great viability in the banking sector and its dynamic and fast expanding level of activities, banks are faced with different kinds of
challenges, among which is trying to prevent various fraudulent intentions of both staff and customers (Bostley & Drover 1992).

Technology (IT) has increased that material exponentially. Whereas advances in technology have improved operations in banks, no equal efforts have been deployed to counter the risks that come from the resulting changes in operations of the banks including complexity of the frauds and forgeries themselves. With the banks focusing on the frauds themselves, they ignore the motives behind the perpetrators of these vices yet their motives are the ones to be tackled if the war on fraud is to be won (Turban et al, 1996). Among the main fraud aspects that these individuals get involved in include cheque fraud, skimming, cloning of credit cards, transfers, forgery, embezzlement and manipulation of the authorized codes. These aspects are easily undertaken with a banking staff member, either directly or indirectly involved. The banking staff, whether while working or having once worked with the bank will not only have the knowledge and skills of how to manipulate systems in order to access sensitive data, but also have confidence to get involved in the malpractices (Vamosi et al, 2010).

EMPIRICAL REVIEW

Know Your Customer (KYC)

The customer is an important stakeholder, and indeed a stakeholder refers to “persons or groups that affect, or are affected by, an organization’s decisions, policies and operations” (Lawrence & Weber, 2008). Financial institutions should not only screen, but know their customers well, obtaining satisfactory evidence of the customer’s identity, and have effective procedures for
verifying the bona fides of new customers. Knowing your customers is really showing Tender Loving Care (TLC) to one’s customers (Low, 2006).

In Kenya, the body patrolling money laundering and fraud has had its powers beefed up. While commercial banks have made steps to combat fraud through implementation of KYC (Know Your Customer) checks and internal controls, the Anti-Money Laundering policy is yet to take effect due to bureaucracy on its implementation by the government. Kenya’s Proceeds of Crime and Anti-Money Laundering (AML) Act, which was signed in December 2009 and came into effect in June 28 2010, aims to enable the identification, tracing, freezing as well as seizure and confiscation of proceeds of crime; giving the Central Bank of Kenya and other law enforcement agencies the power to fight money laundering rather than just monitor it (Gaitho, 2003). The legislation also places the onus on businesses-including casinos, banks and others offering financial services-to do intensive due diligence and keep detailed records on customers and their behavior.

Technology

Institutions are reacting to regulator demands by investing in new systems and processes that make it harder for their institutions to be used for illicit purposes. Nothing can take the place of a well-trained staff, but many of the things that regulators look for are built into AML technology solutions (Beck et al, 2007). For example, the way technology solutions facilitate automation of work flow brings consistency of process and audit-ability. The analytical tools that leverage data from many sources are great for verifying new customers’ identities and performing links analysis. The case for implementing AML technology is strong today and will be stronger still tomorrow. One reason technology makes sense in this context is that the ability to look at transactions together as opposed to one transaction in a vacuum - is critical. This is one of the immediate benefits of moving from a manual process to an automated one, though many institutions continue to grapple with these systems in order to minimize false positives and realize operational efficiencies. Nevertheless, the challenges for AML technology do not appear to be dimming the institutional view of vendors in this market (Beck et al, 2007).

Internal Controls

Once the identification and verification procedures have been completed and the client relationship is established, commercial banks and other FSCs should control the conduct of the account/relationship to ensure that it is consistent with the nature of business stated when the account/relationship is opened (Uglow, 1997). Moreover, commercial banks and other FSCs are expected to have systems and controls in place to monitor on an ongoing basis the relevant
activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for commercial banks and other FSC’s to be vigilant for any significant, unexpected and unexplained change in the behavior of an account or inconsistencies in amount, origin, destination, or type with a customer’s known legitimate activities.

Anti-Money Laundering Act

Kenya finally has an anti-money laundering law: The Proceeds of Crime and Anti-Money Laundering Bill, 2009 received presidential assent on the 31st December, 2009 hence making it law. This law is the Proceeds of Crime and Anti-Money Laundering Act, 2009 (the “Act”). The Act seeks to create a comprehensive legislative framework to combat the offence of money laundering in Kenya and to provide for the identification, tracing, freezing, seizure and confiscation of the proceeds of crime among other things. Anti Money Laundering legislation has come a long way since its inception in 2007. The government had published a bill in 2007 and another in 2008, none of which were passed into law during the years they were published. Before the enactment of the Act, money laundering legislation in Kenya was weak and fragmented.

RESEARCH METHODOLOGY

Research Design

Research design is the plan and structure of investigation so conceived as to obtain answers to the research questions. It includes an expression of both the structure of the research problem and the plan of investigation used to obtain empirical evidence on the relationships between the variables of a study (Cooper et al, 2006). The researcher applied a descriptive research design. The study aimed to give more information on a given variable and show relationship between variables. Descriptive study design helps the researcher to understand the root cause of the research problem (Chordiaet, 1997).

Population, Sample and Sampling Techniques

According to Thomas, Nelson, and Silverman (2010), a population refers to a universal set of all elements in which the characteristics under consideration are present. The target population of the study was employees the six commercial banks within Nairobi they include; tier one; KCB and Barclays Bank, tier two; Consolidated bank of Kenya and commercial bank of Africa and
tier three to include ABC bank and Imperial Bank. The study employed stratified random sampling technique in coming up with a sample size of 48 respondents from a total of 120 from specific department in the six banks chosen; this ensured the selected sample is representative of the target population. Mugenda and Mugenda (2003) indicate that for descriptive studies as this one, a sample size of 10% of the accessible population will be adequate. This study utilized a sample size of 40% taking into consideration that most of the questionnaires were administered through interview mode hence expected high success rate.

Data Analysis Technique

Data entry and management was done using Statistical Package of Social Sciences (SPSS) version 180. Then analyzed using both descriptive and inferential statistics. In this study, measures of central tendency were used to give expected summary statistics of variables being studied. These included mean, mode and median. The multiple regression analysis was used to correlate the four independent variables. According to Fraenkel and Wallen (2000) regression is the working out of a statistical relationship between one or more variables. The researcher used multiple regression analysis to show the influence of the independent variables on the dependent variable. The regression equation is as follows;

\[ Y = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \varepsilon \]

Where:

- **Y**-Is the dependent variable (Fraud challenges)
- **\( \beta_0 \)**-the regression model constant (Y-intercept)
- **\( \beta_1, \beta_4 \)**-Beta coefficients of the explanatory variables
- **\( X_1 \)**-Crime and Anti-Money Laundering (AML) Act
- **\( X_2 \)**-Know Your Customer (KYC)
- **\( X_3 \)**-Technology
- **\( X_4 \)**-Internal controls
- **\( \varepsilon \)**- The error term assumed to have zero mean and independent across time periods.
RESEARCH FINDINGS

Legal Framework on Fraud

From the study findings, most of the organizations have banks have a set process to review and, where appropriate, update customer information relating to high risk client information. On the same, the study established that there was set legal and regulatory compliance program that includes a designated officer that is responsible for coordinating and overseeing the AML framework and that there are written policies documenting the processes that they have in place to prevent detect and report suspicious transactions.

Know Your Customers

To the objective of Know Your Customers, the study found that most of the organizations access personal and private information such as the driving License, customer personal identification such as full names, date of birth, ID number, mobile number, Pin & address of all partners to mitigate fraud.

Internal Controls

On application of Internal Controls, the study established that commercial banks are major institution that are responsible for controlling accounts conducts and relationship while FSC’s were ranked second. However, inadequate auditing and placing too much trust on key employees could result a high risk of frauds and money laundering. Procedure, set regulations and system controls were some of the internal control measure adopted by various bank in combating fraud where Central Bank of Kenya collaborate with commercial banks in controlling fraud and money laundering fully by giving guidelines and procedures that controls money transaction and other rules that enables organization to control fraud.

Technology application

To the objective of Technology application, the survey found that most Real Time Gross Settlement (RTGS) mode of payment is associated with less frauds compared to manual methods of payments and that Pre-printed cheques and customized cheques are less associated with fraud compared to manual cheques where IT adoption assist in combating fraud to a great extent.
Inferential Analysis

To compute the correlation between dependent variable and the independent variables the study conducted and model summary.

Coefficient of Correlation

To compute the correlation (strength) between the study variables and their findings the study used the Karl Pearson’s coefficient of correlation (r). From the findings, it was clear that there was a positive correlation between fraud strategies adopted and Legal framework with correlation value of (0.523), Know your customer with correlation value of (0.614), Internal Control with correlation value of (0.746) and Technology with a correlation value of (0.521). This shows that there was a positive correlation between fraud strategies adopted and Legal framework, Know your customer, Internal Control and Technology application. The finding also infers that Internal Control contribute most to combating fraud followed by Know your customer then Technology application while Legal framework contributed little to combating fraud.

Table 1: Coefficient of Correlation

<table>
<thead>
<tr>
<th></th>
<th>Fraud Strategies</th>
<th>Legal Framework</th>
<th>Know Your Customer</th>
<th>Internal Control</th>
<th>Technology Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Strategies</td>
<td>Pearson Correlation</td>
<td>1.0000</td>
<td>.5230</td>
<td>.6140</td>
<td>.7460</td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td></td>
<td></td>
<td>.0032</td>
<td>.0021</td>
<td>.0043</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>Pearson Correlation</td>
<td>.5230</td>
<td>1.0000</td>
<td>.3420</td>
<td>.1240</td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>.0032</td>
<td></td>
<td>.3421</td>
<td>.0621</td>
<td>1.0000</td>
</tr>
<tr>
<td>Know Your Customer</td>
<td>Pearson Correlation</td>
<td>.6140</td>
<td>.3421</td>
<td>1.0000</td>
<td>.0032</td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>.0021</td>
<td>.0014</td>
<td></td>
<td>.0043</td>
<td>.0172</td>
</tr>
<tr>
<td>Internal Control</td>
<td>Pearson Correlation</td>
<td>.7460</td>
<td>.1240</td>
<td>.0621</td>
<td>1.0000</td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>.0043</td>
<td>.0120</td>
<td>.0043</td>
<td></td>
<td>.0031</td>
</tr>
<tr>
<td>Technology Application</td>
<td>Pearson Correlation</td>
<td>.5210</td>
<td>.3420</td>
<td>.0000</td>
<td>.1660</td>
</tr>
<tr>
<td>Sig. (2-tailed)</td>
<td>.0172</td>
<td>.0031</td>
<td>1.0000</td>
<td>.0031</td>
<td></td>
</tr>
</tbody>
</table>

Coefficient of Determination

The four independent variables (Legal framework, Know your customer, Internal Control and Technology application) that were studied, explain only 66.4% of the fraud strategies adopted as...
represented by the adjusted $R^2$. This therefore means that other factors not studied in this research contribute 33.6% of the fraud strategies adopted. Therefore, further research should be conducted to investigate the other fraud strategies adopted (33.6%) that assists in combating fraud.

Table 2: Model Summary

<table>
<thead>
<tr>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.815</td>
<td>0.664</td>
<td>0.314</td>
<td>0.4211</td>
</tr>
</tbody>
</table>

**CONCLUSIONS**

The study concluded that legal framework assist in combating fraud where organizations have set process to review and update customer information relating to high risk client information. On the same the study concluded that legal Framework set by organizations and central banks such as verification of client personal information assist in combating fraud to a great extent.

Know Your Customers was adopted by banks where most of the banks had access to personal and private information such as the driving License, customer personal identification such as full names, date of birth, ID number, mobile number, Pin & address of all partners to mitigate fraud. Likewise, the study concluded that know your customer strategy assist in combating fraud to a great extent.

To the objective of Internal Controls, the study concluded that commercial banks are major institution that are responsible for controlling accounts conducts and relationship. Inadequate auditing and placing too much trust on key employees could result a high risk of frauds and money laundering. Inclusively, the study concluded that Central Bank of Kenya collaborate with commercial banks in controlling fraud and money laundering fully by giving guidelines and procedures that enables organization to control fraud to a great extent.

Technology have been embraced by banks where Real Time Gross Settlement (RTGS) mode of payment was associated with less frauds compared to manual methods of payments and that Pre-printed cheques and customized cheques are less associated with fraud compared to manual cheques where IT adoption assist in combating fraud to a great extent.
RECOMMENDATIONS

Based on the objectives of the study, the following recommendations were reached. On the Legal Framework on Fraud, the study recommended that employees in all departments to be conversant on set procedures, rules and guidelines in fraud mitigation in order to ensure cases of fraud are zero. On the same the study recommended that all banks to have a fraud risk officer who will be responsible of interpreting fraud and anti-money laundering policies to the employee so that to ease their understanding on the policies.

To the objective of Know Your Customers, the study recommended that rules and guideline lines set by the central banking in financial institution such as personal information and other legal requirement should be adhered to ensure fraud cases are mitigated to zero. On the same the study recommended that personal information of the clients such as PIN should be confidential and electronic gadgets that are placed for the purpose of transaction should be free from retrieving previous gadget used PIN so that to minimize cases of fraud in individuals accounts.

On the objective of Internal Controls, the study recommended that organization should not place too much trust on key employees and that they should conduct adequate auditing on the system so as to mitigate risk. On the same the study concluded that guidelines and procedures provided by the central bank of Kenya in controlling fraud and money transaction are fully adhered in the operation of the bank in all departments to ensure no fraud cases are reported hence precise performance.

To the objective of technology application, the study recommended that prior measures to be set by organization to ensure that relevant fraud related to technology application are mitigated as ignorance to this advancement in implementation of critical strategy such as mitigating fraud will led to low performance of the organization. On the same the study recommended that all staffs to be taught on application of IT in fraud mitigation practices so that all departments can apply the same to identify and mitigate the same.

REFERENCES


International Monetary Fund (2003).


Mugo J. (2010). Assessing the risk in Banking, Kenya Bankers Association, Nairobi


Nduku, M. S. (2007). Credit risk management practices by pharmaceutical companies in Kenya, *Unpublished MBA Project, University of Nairobi*


Vamosi, R., Monahan, M. & Kim, R. (2010). The 2010 Identity Fraud Survey Report,