STRATEGIC RESPONSES ADOPTED BY SAFARICOM LIMITED IN KENYA TO ADDRESS FRAUD RELATED CHALLENGES IN THE M-PESA SERVICE

BY

DAMARIS MUMBI NDUNG'U

A Research Project Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of Master of Business Administration, Department of Business Administration, School of Business, University of Nairobi.

NOVEMBER, 2012

DECLARATION

STUDENT'S DECLARATION

This research project is my original work and has not been presented for a degree in any other university.

Signature……………………………………………..Date……09/11/2012…………………

NDUNG'U DAMARIS MUMBI

D61/63185/2010

SUPERVISOR'S DECLARATION

This research project has been submitted for examination with my approval as University Supervisor.

Signature……………………………………………..Date……09/11/2012…………………

PROF. MARTIN OGUTU

Associate Professor

Department of Business Administration

School of Business

University of Nairobi

ACKNOWLEDGEMENT

I would like to extend my sincere appreciation to all those who contributed to the success of this study. My gratitude goes to University of Nairobi for giving me a chance to pursue this course.

My supervisor Prof. Martin Ogutu deserves a special mention for his professional and academic guidance. His experience and patience came in handy.

I also wish to thank my comrades for their moral and spiritual support. Finally, I thank my dear friends and family members for their continued support in completing this work.

DEDICATION

This research project is dedicated to my late brother Wilfred Mwaura, my loving parents Gladys and Charles, my sister Purity and fiancé Brian who have supported me thus far.

ABSTRACT

Prior studies have found that failure to actively combat fraudulent activity affects organization reputation negatively. At the time of study, only two studies were found that focused on strategic responses adopted by banks in Kenya to counter increasing fraud risks. There was no study that was found focusing on strategic responses adopted by mobile money transfer operators to combat fraud. This is despite the ever increasing cases of fraudulent activity reported by mobile money transfer users and thus calling for strategic responses to curb the spread of the crime. The study generally sought to determine the strategic responses adopted by Safaricom limited in Kenya to address fraud related challenges in the M-PESA service. This was a case study since the unit of analysis was one organization. Primary data was collected using an interview guide which contained open-ended questions. Content analysis was then used to present the data. The information was presented in a continuous prose. The study found that fraud is very sensitive and that customers have an immense fear of falling victim to fraud. The study established that Safaricom has encountered instances of customers using the M-PESA service being defrauded. The study then found that hoax text messages, extortion messages and customers conned to send money are the most prevalent fraud trends in the mobile money transfer service. M-PESA agents were also found to have fallen victim to fraudulent activity. The study found that the organization has dealt strategically with these cases by monitoring transactions for any suspicious activity on a regular basis and putting in place a fraud policy. The study recommends that the organization needs to work closely with law enforcement agencies and various arms of government to come up with policies and structures that deter future fraud incidences. The study further recommends that more research needs to be done on new technological advances and other strategic responses that could help in combating fraud more effectively.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Ansoff and Mcdonell (1990) state that continued organization survival depends on its ability to secure rewards from its environment which replenishes the resources consumed in the conversion process and also ensures social legitimacy. They further argue that a major escalation of environments turbulence in the 1990s has meant a change from a familiar world of marketing and production to an unfamiliar world of new technologies, new competitors, new consumer attitudes and new dimensions of social control. In the space of a decade, mobile networks have become a significant part of the infrastructure in many developing countries." Mobile money" is money that can be accessed and used via mobile phone. The risks that are inherent in all retail payments systems are also present in the mobile space, including money laundering, privacy and security, consumer protection, fraud, and credit and liquidity risks.

Fraud is a million dollar business that is increasing every year. All stakeholders conducting business have an interest in preventing, detecting and mitigating fraud in the organizations. In recent times, a substantial number of individuals have fallen victim to fraudsters targeting mobile money transfer users. These points to the fact that criminal syndicates have identified a loophole in the system that is being exploited to perpetuate fraudulent activity against users. Corporate entities involved with financial transactions have invested a significant amount of resources in mitigating risk and the possibility of fraudulent transactions. When developing their platforms, firms also invest heavily in implementing security features to preserve trust in the system.

1.1.1 Strategic Responses

Strategy refers to a plan of action designed to achieve a particular goal. Strategy is the match between an organization resources and skills and the environmental opportunities it wishes to accomplish. It is the process by which managers set an organizations course, develop plans in the light of internal and external circumstances and take appropriate action to reach those goals. This action refers to the strategies employed in meeting a firm's short term and long term objectives (Johnson & Scholes, 2002). Pearce and Robinson (2005) defined strategic responses as the set of decisions and actions that result in the formulation and implementation of plans designed to achieve a firms objectives. Ansoff and Mcdonnell (1990) noted that strategic responses involve changes in the firm's strategic behaviors to assure success in transforming future environment. Response of any organization can be either operational or strategic. Operational responses are concerned with efficiency of operations while strategic responses are long term in nature, embrace the whole organization, and involve large amounts of resources. Decisions relating to strategic responses are usually made at corporate and business levels of the organization.

Organizational change emphasizes the importance of translating strategic change into detailed resource plans, critical success processes and everyday communication. Corporate strategy is concerned with choices and commitments regarding markets, business and the very nature of the company itself. The strategic response may involve changes in organization's products or services, organization structure, culture and leadership as well internal systems and processes (Johnson & Scholes, 2002).

Strategic leadership is multifunctional, involves managing through others, and helps organizations cope with change. As those business strategies shift, new organizational capabilities are required to implement operational strategies. Organizational structure is all the people, positions, procedures, processes, culture, technology and related elements that comprise the organization. This structure must be totally integrated with strategy for the organization to achieve its mission and goals (Mcguire, 2003).

1.1.2 Fraud Related Challenges involved in Money Transfer

Money Transfer Services refer to services in which money or funds can be transferred from one location to another with the help of various methods. A large number of reputed companies offer a variety of money transfer services to customers. The methods are quick, dependable, and easy to process, with which money can be sent or received all over the world. The operations of money transfer companies are carried out with the help of the extensive network of agents' networks and actively engaged companies in this sector. These services include online money transfer services where money or funds are transferred over the internet (Wishart, 2006).

Forms of money transfer services include but are not limited to: "walk in" money transfer services where cash is received from the customer by a clerk and the payment is ready for collection at an agent location, suitable for the receiver. Telephonic money transfer services allow funds to be sent telephonically by utilizing a debit card or credit card. Payout services allow receivers to collect funds within a short period of time after the sender has completed the transaction. Money orders are a dependable payment option used for bill payments and various purchases.

Prepaid cards and services can be used as automated teller machines cards or for online shopping purposes wherever the cards are acknowledged. Mobile money transfer services are used to transfer funds from one person to another by using mobile phone numbers (Merritt, 2010).

Fraud can be defined as all multifarious means which human ingenuity can devise, and which are resorted to by an individual to gain advantage over another by false suggestions or suppression of the truth. Fraud encompasses an array of irregularities and illegal acts characterized by intentional deception either for the benefit or detriment of the organization by internal or external parties. The threat of fraud is faced by all organizations regardless of their size or sector. From the perspective of reputation management, controlling the impact of fraud is particularly challenging because it implies that an organizations compliance systems are vulnerable (Bartlett and Ballantine, 2002). Money transfer services are often the preferred method used to obtain cash by a variety of fraudsters. Money transfer services allow individuals to send cash quickly, easily and reliably, this attracts criminals to obtain cash from users fraudulently through well orchestrated scams. When money transfer services are being used in connection with criminal activity, the recovery of any cash sent is extremely difficult (Whitman, 1991). Money transfer services are often used by fraudsters in connection with many types of fraud including advance Fee Fraud which means paying money for a promise of wealth (419 Fraud), criminal cash-back, cheque/draft overpayments, shipping and escrow frauds, high yield investments, share and other investment frauds, identity fraud ,internet, advertising, auction and on line fraud (www.met.police.uk).

1.1.3 M-PESA Service in Kenya

In March 2007, following an initial pilot co-funded by Vodafone and the United Kingdom’s Department for International Development (DFID) Financial Deepening Challenge Fund, Safaricom (the Kenyan Vodafone affiliate) launched M-PESA, a mobile-based payment service (Ignacio et al., 2010). The product is called M-PESA since “Pesa” is the Swahili word for money and the “M” is for mobile. M-PESA is a short messaging service based system that enables users to deposit, send, withdraw funds, pay bills, buy airtime and buy merchandise using their mobile phone. Customers do not need to have a bank account and can transact at any of the country wide agent outlets. Registration and deposits are free and most other transactions are priced based on a tiered structure to allow users to be able to use the system at a reasonable cost (FSD Kenya, 2009).

The top three factors that help to explain the success of mobile transactions in Kenya are the impressive adoption of mobile phones, the need to access financial services, and the low cost of mobile money transfers. Originally, M-PESA intended just to design and test a platform that would allow customers to receive money and repay small loans using their handsets. The service was also designed to help microfinance institutions streamline their operations, raising efficiency and boosting business growth. It has certainly achieved these objectives. But other, unexpected, uses have also emerged. They indicate that a service like M-PESA has the potential to be extended in many innovative ways (Omwansa, 2009).

1.1.4 Safaricom Limited M-PESA service

Safaricom Limited was formed in 1997 as a fully owned subsidiary of Telkom Kenya. In 2000, Vodafone group Plc of the United Kingdom, acquired a 40% stake and management responsibility for the company. Since launching M-PESA in September 2007, Safaricom has signed up more than eight million people to M-PESA. A year after the launch, there were 1.6 million registered users and a network of over 1,200 agents where people could register, deposit, and withdraw money (FSD Kenya, 2009). Safaricom has developed an impressive local team to manage M-PESA operations. The team consists of individuals from Finance, Customer Care, Product Management, Sales and Marketing that are dedicated to ensuring M-PESA runs smoothly. In addition to the Safaricom team, the external agency hired to manage the agent network regularly relies on their staff to train and visit agents. Vodafone Global Services has also developed a wide-scale team that is dedicated to supporting M-PESA in countries where it has already launched as well as the on-going development and roll out of the service in other countries (Ignacio et al., 2010).

According to Ignacio et al. (2010), revenue on M-PESA transactions is on average 4.3 times greater than that of airtime commission earned by agents. Incentivizing the agent network is an essential component to ensuring their co-operation and ongoing commitment to delivering quality service. Customers use a PIN when processing transactions and are required to repeat a secret password when they call customer care. All transactions are securely encrypted by the SIM application toolkit so there is little risk of interception when the messages are being transmitted. Reconciliation between the M-PESA system balance and the bank account where cash is held is done through a careful procedure that requires multiple members of the M-PESA team to validate and sign off daily (Safaricom, 2007c).The Central Bank of Kenya is actively involved in the regulation of mobile money services in Kenya. In early 2008 the Central Bank of Kenya announced that they would be performing a full audit of the MPESA system. After months of closely following M-PESA procedures and monitoring transactions, the Central Bank of Kenya was satisfied with the operation of the system (Omwansa, 2009).

1.2 Research Problem

Pearce and Robinson (2005) defined strategic responses as the set of decisions and actions that result in the formalization and implementation of plans designed to achieve a firm's objectives. Well developed and targeted responses are formidable weapons for a firm in acquiring and sustaining competitive edge (Ansoff & Mcdonell, 1990). Fraud is believed to be amongst the most serious corporate problems and challenges in today's business environment. Fraud or scam is a dominant white collar crime; common fraud types include cheque fraud, computer fraud and internet fraud (Palshikar, 2002). It is important for organizations to respond appropriately to fraudulent activities because loss of revenue is only the immediate issue involved in not dealing with fraud proactively. Lack of customer faith and of perceived security lead to long-term loss in revenue and the inability to stay competitive in a quickly changing market (GSMA 2008c).

Safaricom Limited is a leading mobile network operator in Kenya. It was formed in 1997 as a fully owned subsidiary of Telkom Kenya. In May 2000, Vodafone group Plc of the United Kingdom, the world's largest telecommunication company, acquired a 40% stake and management responsibility for the company (Safaricom, 2007c). In March 2007, Safaricom launched M-PESA, a mobile-based payment service (FSD Kenya, 2009).

The research will focus on this mobile payment provider because it was the first to be introduced in the country and has more subscribers than any other in Kenya. Fraud or conning is an issue of great concern for Safaricom and M-PESA, because fraudsters are continuously coming up with new ways of conning unsuspecting Safaricom and M-PESA customers and getting money from them. Safaricom has invested a significant amount of resources in mitigating risk and the possibility of fraudulent transactions. When developing the platform, Vodafone invested heavily in implementing security features to preserve trust in the system (Safaricom, 2007c). However, the strategies used so far to combat fraud have only been successful in eliminating fraudulent activity to some extent and this continues to be a persisting issue. This study will seek to establish how Safaricom is dealing with fraud related challenges in its mobile money transfer service.

Fraud appears to be an area that is not quite researched. Only two studies were found that looked at fraud related issues. A study by Cheptumo (2010), investigated strategic responses to fraud related challenges by Barclays Bank of Kenya. The study found that fraud is very sensitive and that customers have immense fear of fraud and that it impacts negatively on banks profitability. Cheptumo recommends that a review of fraud legislation could reduce fraud related risks in the banks. The other study was by Wanemba (2010), who studied strategies applied by commercial banks in Kenya to combat fraud and found that, majority of the causes of fraud are related to an advance in technology. Wanemba proposed that banks should ensure that they employ the latest technology to strengthen their internal controls hence reducing fraudulent activity. The current study differs from that of Cheptumo (2010) because while Cheptumo looked at strategic responses to fraud related challenges in the banking industry, the current study looks at M-PESA which is a relatively new phenomenon. M-PESA operations are quite different from the way banks operate and hence the findings of Cheptumo may not be used to generalize on strategic responses to fraud related challenges in the M-PESA service. The questions that will be addressed in this study will be: what are the fraud related challenges encountered by Safaricom Limited in the M-PESA service? What are the strategic responses adopted by Safaricom Limited to deal with fraud related challenges in the M-PESA service?

1.3 Research Objectives

The objectives of this study will be:-

i. To establish the fraud related challenges encountered by Safaricom Limited in the M-PESA service.

ii. To determine the strategic responses adopted by Safaricom Limited to deal with fraud related challenges in the M-PESA service.

1.4 Value of the Study

Compliance with anti-crime laws is a challenging proposition for money transfer services globally because it represents unfamiliar territory to the telecommunications industry (GSMA 2008c). The telecommunications industry in most countries is regulated on the basis of a public utility, whereas the banking sector is regulated on the basis of safety and soundness and capital adequacy. The aim of this study is to identify fraudulent activity and determine the strategic response by the mobile network operator to fraud challenges arising from mobile operator payment service (M-PESA).

There are risks more unique to telecommunications firms that financial institutions and their regulators lack experience in detecting and monitoring. The conjoining of telecommunications and banking sectors will require a new cooperative regulatory environment across industries and geographical jurisdictions to employ risk-based and proportionate oversight (Merritt, 2010). Money transfer service providers especially in the mobile money transfer services will get insights on the fraud trends currently being used by con artists to defraud their customers and how to respond appropriately.

Findings of this study should be useful to the Communications Commission of Kenya (CCK) should they wish to review the mobile money transfer regulatory policies. New regulatory policy will require a comprehensive understanding of the new risks that mobile transactions introduce to consumers, including lost payments through fraudulent transactions, identity theft, or criminal activity (GSMA, 2007). Scholars and the society at large stand to benefit as a result of increased awareness through routine communication on payment system risk issues on the media platforms, social media, government publications and academic research. The findings could also benefit future researchers, by providing a base on which further studies could be done.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter consists of the review of existing literature that is relevant to the study. The specific areas covered here are organizations and the environment, strategic responses, money transfer services, fraud in money transfer services and combating fraud in money transfer services.

2.2 Organizations and the Environment

According to Thompson (1997), for a firm to control its growth, change and development, it must seek to control the forces which provide the opportunities for growth and those that pose threat. In a turbulent environment, the organization must change its strategies and possibly its beliefs so as to maintain environment values resources (EVR). Strategic diagnosis identifies whether a firm needs to change its strategic behavior to assure success in its future environment. If the need is confirmed, the next thing would be to select and execute specific actions which may bring the firms aggressiveness and responsiveness in line with the environment (Ansoff, 1990). Ansoff further explains that there has to be an appropriate transformation of a firm's capability to match the changed environment. These changes may involve the human resource, management, finance, operating systems and policies that guide the firm's strategic thrusts.

To be successful overtime, an organization must be in tune with its external environment. Pearce and Robinson (2005) show in their model that the external environment consists of two interactive and interrelated segments, these are the operating environment and the remote environment. The operating environment consists of competitors, customers, creditors, labor market and suppliers that are the immediate business environment. The remote environment consists of the economic, political, social, ecological and technological aspects. There is need to understand an industry's dominant features which include market size, growth rate and the scope of competitive rivalry (local, regional, national, global).

Pearce and Robinson (1991) also state that drivers of change in an industry include changes in growth rate, consumer behavior, product innovation, technological change, marketing innovation, increasing globalization and changes in government policy. Two frameworks are used to analyze the environment; Political, Economic, Social, Technology, Ecological, Legal (PESTEL) and Strength, Weakness, Opportunity, Threat (SWOT) analysis. Chege (2008), states that volatility of external influences how organizations restructure themselves to cope with changes or how to anticipate changes. PESTEL analysis is often carried out by management to enable them to develop informed strategies on long term plans.

Pearce and Robinson (2005) observed that the direction and stability of political factors are major consideration for managers when formulating strategy. This is because the administrative and legal environment in a country provides a framework within which every organization operates. They argue that every firm must consider the economic trend not only at a national level but also internationally. Economic analysis should centre on aspects like inflation rates, economic growth rate, availability of credit, level of disposable income and propensity to save on credit. Technological breakthroughs can have sudden and dramatic effects on the environment; all firms should keep up with new technology to compete effectively. Social factors that affect organizations involve the beliefs, values, attitude and lifestyles of persons in the firm's external environment. Firms should always align their strategies to counter changes from these social factors. According to Ansoff and McDonnell (1990), fundamental forces of change have been experienced in the global business environment resulting in unprecedented competition. Effective strategy may enable a business to influence the environment in its favor and even defend itself against competition. Porter (1985), states that a firm must formulate a business strategy that incorporates cost leadership, differentiation or focus in order to achieve a sustainable competitive advantage in the industry.

An organization's internal environment is composed of the elements within the organization which consist of current employees, management, corporate culture and organization structure. It is imperative for the organization to conduct an internal analysis to obtain a clear picture regarding its strength and weaknesses, opportunities and threats. Based on these, the organization can devise suitable strategies to leverage strengths and overcome its weaknesses (Martin, 2010). The organization's mission statement describes what it stands for, why it exists and explains the overall purpose and its unique attributes that distinguish it from others. Company policies form guidelines that govern how situations are addressed. Formal structures are hierarchical arrangement of tasks and people which determines how information flows within the organization. The culture of the organization is its personality just as each individual has a distinct personality. Resources are the people, information, facilities, infrastructure, machinery, equipment, supplies and finances at the organization's disposal. The strategic management process results in decisions that can have significant long lasting consequences. Erroneous strategic decisions can inflict severe penalties and become exceedingly difficult if not impossible to reverse. The responsiveness of the organization's capability must be matched to the environmental turbulence (Angara, 2010).

2.3 Strategic Responses

Strategy is the direction and scope of an organization over the long term which achieves advantage through its configuration of resources within the changing environment and fulfills stakeholder's expectation (Johnson and Scholes, 2002). Strategy is a multi dimensional concept that embraces all critical activities of the firm, providing it with a sense of unity, direction and purpose as well as formulating the necessary changes induced by its environment (Martin, 2010). Strategic responses are the set of decisions and actions in the formulation and implementation of plans designed to achieve a firm's objective. Strategic responses involve changes to the organization's behavior (Pearce and Robinson, 2005). Ansoff and McDonnell (1990) described four primary types of responsiveness which serve a distinct goal for the firm. Operating responsiveness aims at minimizing the operating cost of the firm, competitive responsiveness optimizes the firm's profits, innovative response develop profit potential and entrepreneurial responses develop the organization's long term profit potential. In business strategy, strategic intent means leveraging the firm's internal resources, capabilities, and core competencies to accomplish goals in the competitive environment. Typically, core competencies relate to the functional skills of an organization, such as manufacturing, finance, marketing, and research and development (Abdalla et al., 1998).

The usefulness or relevance of a response adopted by a firm is measured by how well it has countered the challenges emanating from the external and internal environment.

Porter (1985) noted that information technology can create new businesses from within a company's existing activities. Thompson (1997) observed that a good financial strategy involves providing the firm with the appropriate financial structure and funds to achieve overall business objectives and careful examination of financial implications of various strategic options such as acquisitions or investments. Thompson (1994), states that human resources are an essential strategic resource because people are needed to implement strategies and to this they must share the objectives and values of the organization. Wheelen and Hunger (1998) define research and development strategic response as a process that deals with products, services and processes innovation and improvements. A firm that is consistently carrying out R&D ensures consistent addition of value to the existing products or services or creation of new products or services.

Organizations align their value chains to create manufacturing, marketing, and human resource strategies. In other words, structure shapes strategy. In order to reach strategic objectives and address industry problems, companies need effective leadership that is founded upon vision and communication. As strategic leaders, corporate managers make decisions intended to help their firm develop, maintain, strengthen, leverage, and exploit core competencies. In general, the most effective core competencies are based on intangible resources, which are less visible to competitors because they relate to employees' knowledge or skills (Abdalla et al., 1998). Thompson, Strickland and Gamble (2007) state that corporate culture is the organizations personality as shaped by its core values, beliefs, business principles, traditions , work practices and styles of operations.

Forces that cause the corporate culture to evolve are new challenges in the market place, revolution of technologies and shifting internal conditions. Ansoff and McDonnell (1990) assert that the strategic response is initiated once the rational trigger point is reached. This is the point at which accumulated data shows that there is a serious decline in performance which cannot be reversed and special counter measures are required.

2.4 Money Transfer Services

Money Transfer Services refer to services in which money or funds can be transferred from one location to another with the help of various methods. In money transfer, an order is placed with a financial institution or wire-transfer service provider to disburse funds a person has provided to another party. In most countries, retail payment systems have been dominated by banks whose primary function in the most basic sense is to gather deposits for deployment in loans and other permissible investments. Banks and wire transfer providers have networks of affiliated financial institutions or agents worldwide that complete the requested transfer of funds on a person's behalf, usually for a modest fee (GSMA, 2008). Today the majority of money transfers are carried out by electronic funds transfer (EFT) using the internet. Examples of money transfer services include but are not limited to: money order which is a payment order for a pre-specified amount of money. PayPal is a global e-commerce business allowing payments and money transfers to be made through the Internet. Telephonic money transfer services allow funds to be sent telephonically by utilizing a debit card or credit card. Mobile money transfer services are used to transfer funds from one person to another by using mobile phone numbers. Person-to-person (P2P) payments are evolving to the next generation of electronic payments using the mobile channel. They are supporting a new and viable channel for mobile financial services, including bill payment and account transfers, domestic and international person to person transfers, proximity payments at the point of sale, and remote payments to purchase goods and services (Merritt, 2010).

Some of the regulatory challenges particularly in money transfer were summarized after a meeting in Malaysia between regulators from Asia Pacific countries, providers and international organizations. Some of the challenges for regulators were: Allowing non-bank third parties, such as local merchants, to conduct "cash-in/cash-out" functions and to interact directly with customers and to perform 'Know Your Customer' procedures for remote account opening. Adopting the right measures to address money laundering and combating the financing of terrorism under the Anti-Money Laundering and Anti-Terrorism Financing Act (AMLAFA) of 2001. Ensuring effective consumer protection to avert potential issues that may arise with the use of mobile phones and the use of agents, including issues such as privacy and fraud. Identifying the right regulatory space for the issuance of e-money and other stored-value instruments (particularly when issued by parties other than licensed and supervised banks).Allowing an appropriate balance of competition and cooperation in retail payment systems in order to promote a certain degree of interoperability (Bank Negara Malaysia, 2009).

The main challenges when it comes to distribution in money transfer services include: Reliability where concerns have been expressed regarding the quality of procedures outsourced to agents and the robustness of controls (account opening, client identity validation), there has also been concerns about control over or trustworthiness of staff. External staff competence needs to be monitored to ensure their level of training and competence. Security in as far as cash is concerned; banks and agents must ensure that funds are sufficiently protected from theft. Servicing remote agents with wholesale cash services can be very risky and costly. Continuity is a concern where agents may go out of business or terminate distribution agreements (Singh and Shelly, 2010). Mobile operators face operational constraints due to restrictions on cross border trade in retail financial services, currency convertibility and differences between national legislative and regulatory frameworks that erode opportunities for economies of scale to be achieved in a cross-border environment. In cross border context, authorities are most concerned to stem money laundering and terrorist financing and hence most strictly apply customer due diligence rules (Schutts, 2007).

2.5 Fraud in Money Transfer Services

Fraud is defined by the Malaysian Approved Standards on auditing (2001), AI No. 240 as an intentional act by one or more individuals among management, employees or third parties which results in a misrepresentation of financial statements (Cheptumo, 2010). Concise English dictionary defines fraud as an act of deceit, scam, con, cheat, hoax, scandal by means of false representation to obtain an unjust advantage. 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. Fraud can be committed through many methods including mail, wire, phone and the internet. The difficulty in checking identity and legitimacy online, and the ease with which hackers can divert browsers to dishonest sites and steal credit details and the ability for users to hide their location all contribute to making internet and mobile fraud very fast growing. Every day, many types of consumer fraud result in losses to gullible consumers. Promises that they will get rich quick lure unsuspecting consumers to part with their cash (Whitman, 1991).

funds are sufficiently protected from theft. Servicing remote agents with wholesale cash services can be very risky and costly. Continuity is a concern where agents may go out of business or terminate distribution agreements (Singh and Shelly, 2010). Mobile operators face operational constraints due to restrictions on cross border trade in retail financial services, currency convertibility and differences between national legislative and regulatory frameworks that erode opportunities for economies of scale to be achieved in a cross-border environment. In cross border context, authorities are most concerned to stem money laundering and terrorist financing and hence most strictly apply customer due diligence rules (Schutts, 2007).

2.5 Fraud in Money Transfer Services

Fraud is defined by the Malaysian Approved Standards on auditing (2001), AI No. 240 as an intentional act by one or more individuals among management, employees or third parties which results in a misrepresentation of financial statements (Cheptumo, 2010). Concise English dictionary defines fraud as an act of deceit, scam, con, cheat, hoax, scandal by means of false representation to obtain an unjust advantage. 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. Fraud can be committed through many methods including mail, wire, phone and the internet. The difficulty in checking identity and legitimacy online, and the ease with which hackers can divert browsers to dishonest sites and steal credit details and the ability for users to hide their location all contribute to making internet and mobile fraud very fast growing. Every day, many types of consumer fraud result in losses to gullible consumers. Promises that they will get rich quick lure unsuspecting consumers to part with their cash (Whitman, 1991).

According to Wanemba (2010), challenges of fraud in organizations can be dealt by communicating with employees changes regarding fraud related issues before the strategy implementation has already been crystallized. Organizations need to invest on training employees on what fraud is, how to combat fraud and ways in which to prevent fraud occurrence. Another challenge is the improvement and increase in technology which has led to increase in fraudulent activity due to the use of software used to access unauthorized information and disguise location of the fraudsters. Lack of proper infrastructure makes it very difficult to trace fraudulent activity and apprehend the accomplices. Fraud impacts negatively on a company's reputation which in turn may result in dipping revenues due to loss of customer confidence.

2.6 Combating Fraud in Money Transfer Services

According to Cheptumo (2010), the risk of fraud should be included on the agenda of every corporate strategy planning meeting. Systems and controls should be examined to identify weaknesses which make the company susceptible to the risk of fraud. Once the risks are identified, a gap analysis can be completed and improvements recommended mitigating the risk of fraud then subsequent monitoring should ensue. It is prudent to adopt the best practices in combating fraud. Avenues to report such cases should be available; for instance telephone hotlines and special email addresses that encourage whistle blowing. Perpetrators must be punished to ensure there is a paradigm shift in terms of the culture. The aim of a company's fraud policy is to demonstrate to both employees and other stakeholders that the company is taking the threat of dishonesty, fraud and theft seriously. The methods that the fraud examiner can take to increase awareness of the risks faced by the company include; taking the management and staff through an education process through lectures, presentation of case studies on fraud trends, use of an organization's intranet and articles in company magazines (www.targetmarketingmag.com/article/how-combat-fraud).

Organizations must continuously review and improve their internal controls as the primary defense against fraud and abuse. This involves setting up structures within an organization that have capacity to pick up on fraudulent activity. When fraud has been detected, an organization's main concern is to identify whether it is an internal or external problem. Investigating a case may involve covert operations, surveillance, informants and other sources of information (Apostolou, 2000a). The objective of deterrent security controls is to create an atmosphere of control compliance, preventative security measures are designed to reduce the possibility of an attack. Once the system has been violated, detective controls help in identifying the occurrence of harm and security breach. Corrective measures serve to reduce the impact of the threat after a loss has occurred (Katz, 2000).

According to Merritt (2010), the risk of anonymity in money transfer services may require new authentication technologies such as voice recognition and fingerprinting to verify identification and to employ appropriate know your customer (KYC) programs, particularly at vulnerable points of a transaction where cash withdrawals may be conducted. The use of more sophisticated control systems to flag unusual account activity will be needed to detect increasingly complex money laundering schemes. Education and collaboration across organizational jurisdictions and the telecom and financial services industries will be necessary to detect and mitigate criminal activity, fraud, and other payment system risks. Location based services available in smart phone applications may also help payment service providers to authenticate the credentials of mobile users engaging in payments transactions. Chatain et al (2008) proposes that as domestic and international money transfer services grow more prevalent, discussions on risk management and payment system integrity will be imperative. Dialogue with all industry stakeholders, including regulators and policymakers, is essential to creating an environment in which payments risk issues are clearly understood. In this way, risk-based regulation that is proportionate with the need to encourage innovation and efficiency in retail payments can be best achieved.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1Introduction

This chapter describes the methodology that was used to carrying out the study. It constitutes the blue print for the collection, measurement and analysis of data. It is a plan for selecting the sources and types of information used to answer the research questions and meet the study objectives. The chapter covers the following sections; research design, data collection procedures and data analysis.

3.2 Research Design

Research design provides the glue that holds the research project together. A design is used to structure the research. It shows how the major parts of the research work together to try and address the central research questions (Mugenda and Mugenda, 1999). The research is a case study of the M-PESA service. In the M-PESA service, Safaricom is the main organization with well established systems. Safaricom is the most affected by fraud in the mobile money transfer sector. The study investigated the strategic responses adopted by Safaricom to address fraud related challenges in the M-PESA service.

This research design was chosen because the objectives of the study required an in depth understanding of M-PESA and the specific strategies being applied in adapting the service to the changing business environment. The advantage of using a case study involves an intensive study of the concerned unit which makes it possible to obtain the inside facts from experienced employees.

The importance of a case study was emphasized by Yin (1988) who acknowledged that case studies contribute uniquely to our knowledge concerning the individual, an organization, social and political phenomena. A similar study by (Cheptumo, 2010) successfully adopted this research design.

3.3 Data Collection

The study relied on primary data. Primary data was obtained through an interview guide with open ended questions (see appendix 1). According to Walliman (2005), the use of interviews to question people is a very flexible tool with a wide range of applications. Interviewing is particularly useful when qualitative data is required. The two main methods of conducting interviews are face to face and telephone. In this case study, an interview guide was used to facilitate personal interviews with the target respondents with a view to obtaining in- depth and comprehensive data regarding the variables of the research study. In-depth interviews gather narrative accounts of events, experiences, perception and reality.

The interview guide was semi structured to achieve defined answers to defined questions, while leaving time for further development of those answers and including more open-ended questions. It was broken down into two sections; section one contained the demographic data of the respondents and section two contained the variables of the research study. The interview guide was submitted personally by the researcher to a total of eight respondents. The target respondents included: Senior fraud analysts M-PESA section, Fraud analysts M-PESA section, Team Manager M-PESA section, Support analyst M-PESA section and Customer Operator M-PESA section.

3.4 Data Analysis

Walliman (2005) states that little sense can be made out of a huge collection of data; therefore an essential part of research is the analysis of the data. This analysis must be carried out in relation to the research problem. Data analysis in this case study was done through counter checking the interview results for errors and completeness, then editing and coding was done. Content analysis was used to analyze the qualitative data gathered for both objectives because the respondents were drawn from a single organization.

Kothari (2004) argues that content analysis is a central activity whenever the nature of the study includes verbal materials. It examines the intensity with which certain words have been used, systematically describing the form or content of written and spoken material. The technique used a set of categorization for making valid and replicable inferences from data to their context. Qualitative data was presented through narratives.

CHAPTER FOUR

FINDINGS AND DISCUSSIONS

4.1 Introduction

This chapter presents the results and discussions of the data from the field. The research is a case study of Safaricom limited and is qualitative in nature. It is organized into two parts according to the objectives which are: To establish the fraud related challenges encountered by Safaricom Limited in the M-PESA service and to determine the strategic responses adopted by Safaricom Limited to deal with fraud related challenges in the M-PESA service

4.2 Challenges and Discussions

In this section, interview results regarding the fraud related challenges and strategic responses are presented and discussed.

4.2.1 Fraud Related Challenges experienced Internally in the M-PESA Service

The study sought to know whether Safaricom Limited was experiencing fraud related challenges in its M-PESA service. All of the interviewees of the study indicated that there were various types of frauds that had been reported by their subscribers over a period of time. They stated that fraud is very sensitive and that the subscribers have an immense fear of falling victim to fraud.

The study further sought to find out whether the organization had a fraud policy and how the organization ensures that the employees are conversant with that fraud policy. The response received from all the interviewees was that Safaricom limited has a fraud policy in place. The policy defines fraud in its entirety and sets out strategic direction and objectives for managing fraud risk. The organization ensures that employees are conversant with the policy by sending regular reminders through e-mail to the staff urging them to keep themselves aware on the policy. As well, regular training sessions are held by the Risk and Management division to give guidance and to clarify any concerns that the staff may have regarding the fraud policy.

The interviewees were requested to comment on whether Safaricom has encountered customers being defrauded by employees and the types of fraud challenges experienced internally regarding the M-PESA service. All the interviewees indicated that they had heard reports from official channels in the organization about instances where certain employees defrauded customers. The types of fraud encountered internally by the interviewees include; fraudulent swapping of subscriber lines to obtain funds from the subscribers M-PESA account, sending of start keys fraudulently to enable a fraudster to gain access to the subscribers M-PESA account, soliciting for bribes from potential M-PESA agents to expedite the process of acquiring tills and unauthorized withdrawal of funds from subscribers M-PESA accounts.

The study then sought to know the strategic response that the organization used to deal with past cases of fraudulent activity by employees and to combat fraud within the organization. The interviewees indicated that internal systems and procedures are modified regularly to ensure that the systems are not compromised for fraudulent activity. The M-PESA system operates on a maker-checker authorization process. This means that once a transaction is posted by a person, it can only be authorized by a person of a higher rank which makes it difficult for an employee to act alone in committing fraud. As well, regular screening of employee activity while using the company's systems is carried out to monitor any ongoing suspicious activity. Avenues to report fraud and whistle blowing have been provided. These can be done through an ethics hotline or ethics email addresses as well as direct reporting to the Chief Executive Officer for especially sensitive information. Training sessions are also held regularly to keep employees informed on fraud risks as well as to obtain their participation through feedback on special innovations or procedures to combat fraud. Emphasis is placed on following the Know Your Customer (KYC) procedures to ensure that subscriber information is accurately recorded and available for future reference. Learning material is also readily available in the form of quizzes, case studies on fraud and printed material such as arm bands and t-shirts that are circulated within the organization to ensure that everyone owns the concept of combating fraud.

As part of the strategic response, the recently appointed Chief Executive Officer presented a new organizational structure which created the customer focused Strategic Business Units and streamlined the supporting Corporate Centre. This is fundamentally aligned to Safaricom's strategic direction. The leaner structure presents three Revenue Centers: Financial Services, Enterprise and Consumer business and six Function positions. The Risk division and management division maintained its autonomy while the customer care division was merged with the marketing division.

Safaricom has also demonstrated its flexibility with regard to the corporate strategy by overhauling the existing managerial positions and creating new leaner positions with freshly recruited external and internal employees. A new culture dubbed "Safaricom 2.0" was introduced and is currently being implemented where employees are encouraged to be more flexible in relating with each other. The new culture has resulted in inclusion of employee behavior as part of the key performance indicators. This means that employees have to represent the company as ambassadors while out in the public. The key pillars of this culture are Simplicity, Speed and Trust. As well, employees are required to meet the company's objectives which include fraud prevention for which they receive recognition or reward.

The following findings are consistent with Wanemba (2010) in her academic research to establish the strategic response to fraud related risks by commercial banks in Kenya. In each instance where fraud is detected, management should reassess the adequacy of the current control environment (particularly those controls directly impacting on the fraud incidents) to consider the need for improvements. Internal and external audit provide independent and objective review and advisory service to the Chief Executive Officer and the directors that the financial and operational controls designed to manage the entity's risks are effective. Many entities choose to outsource various aspects of their fraud control arrangements.

4.2.2 Fraud as a Result of External factors

The study then sought to know whether Safaricom experiences fraud as a result of external factors. The interviewees indicated in the affirmative expressing that a large number of the fraud cases reported were in fact as a result of external influence. The study then sought to find out if technology has led to an increase in fraudulent activity in the M-PESA service and how. The responses to these were that technology has led to an increase in fraudulent activity because of the surge in the number of mobile phones in the

Kenyan market, cheaper airtime and the ease in availability of internet access. This has made it easier for fraudsters to operate in the mobile space. One of the controls that have been used by the organization to mitigate fraud has been to conduct investigations and once found to be engaging in fraudulent activity, blacklist the offending subscriber simcard and the handset. However, due to the cheap offering of Safaricom simcards and affordability in mobile phones, the fraudsters are able to continue with their fraud tactics.

The study then enquired as to how the legal/regulatory environment in Kenya impacts on fraudulent activity. The interviewees responded by saying that legal/regulatory environment has been quite helpful in dealing with fraud but indicated that much more needs to be done. For instance, complaints from subscribers indicate that reports to the police department about fraud cases are not acted upon efficiently which lead to fraudsters evading with customer funds. In addition, even after conviction of fraudsters through the court system, the fines and sentences imposed upon the offender are too lenient allowing the fraudsters to get off and continue with the same fraudulent trends. This has led to an increase in fraudulent activity especially from perpetrators of fraud who are already behind bars. The interviewees commented that large numbers of fraudulent activities were traced to prisons around Kenya.

The study then further required the interviewees to comment on how the organization has responded to the factors above. The interviewees responded by saying that Safaricom works hand in hand with the police CID department to assist subscribers by finding and apprehending perpetrators of fraud crimes. The organization has also reached out to the prisons' department to assist in reducing the number of fraud cases, majority of which are as a result of prisoners' illegal activity. Safaricom has signed a Memorandum of

Understanding (MoU) with the Kenya Prisons Service looking to address the mobile phone crime being committed from the confines of the country's prisons. This provides structure to an existing partnership between the Prisons Service and Safaricom. As well, the organization is appealing to the law makers to make more stringent laws that impose longer sentences and harsher fines to deter further cases of fraud. The organization has also modified the simcard to a higher grade quality (SIM 3.5K) with an address look up feature that ensures subscribers do not send money to the wrong recipient.

The introduction of the new Big SIM 3.5K enabled sim card which allows a subscriber to look up the recipient in the contact (address look up) was a big step towards curbing fraud. There were appeals made from the public since the launch of the M-PESA service to have the address look up incorporated in the menu to avoid instances where funds were sent to the wrong number. This was a point of concern for many users who send money to the wrong recipient and funds are then withdrawn without the senders consent. The new feature which was launched early last year (2011) makes it difficult for fraudsters to con the users because the user is able to send money to easily recognizable numbers.

4.2.2.1 Hoax Text Messages from Persons Impersonating Safaricom / M-PESA staff

The study then sought to know whether customers receive hoax text messages from persons impersonating Safaricom/M-PESA staff. The response given by all the interviewees is that there have been reports of customers receiving hoax text messages from persons impersonating Safaricom/M-PESA staff with the intention of conning the customer to send money to the fraudsters. Examples of these hoax messages that are reported consistently include; fake winning messages about nonexistent promotions, fake cargo delivery messages, fake M-PESA messages for transactions that have not been initiated and messages from fake employment recruiting agencies that persuade the customers to send money. The interviewees then indicated that there have been instances as well, where customers sent money to these impersonators believing that they were indeed Safaricom employees.

The interviewees indicated that the organization has dealt with such cases by educating the public through mass media communication on all of Safaricom's promotions and the number that will be used to contact the winners. The organization also places a lot of emphasis on calling their customer care numbers, liaising with the customer care executives through the social media platforms or visiting any of the retail centers to confirm any doubtful information.

4.2.2.2 Line Swapping and Loss of Funds

The study then sought to find out whether customers have been susceptible to having their lines swapped and funds accessed by unknown people. The interviewees responded by saying that there have been cases reported in the past where customer lines were swapped by fraudsters and the money in the M-PESA account withdrawn. This was a result of the customer issuing to the fraudsters their secret pin and other secret information provided to them by the company to ascertain legitimate ownership of the line. This is done through a process called social engineering where fraudsters call the customer and solicit for their secret details while impersonating the organization's employees. The interviewees also stated that the company does try to recover funds lost through fraud but only if the money is available in the recipient's account.

The company has dealt with this problem by reiterating to its subscribers the importance of keeping secret the information that confirms legitimate ownership of the line. This has been done through aggressive campaigns on mass media, social media and its own hotlines that caution the public on revealing their information unless called by Safaricom through their easily recognizable numbers. Safaricom has referred aggrieved customers who have lost funds through such means to report to the CID police department who will then work with the company to try and apprehend the offender.

Wanemba (2010) in her study looked at the effectiveness of Know Your Customer (KYC) policies adopted by commercial banks in Kenya in reducing money laundering and fraud incidences. In her findings, banks that fully complied with the policy reported fewer cases of fraud. Therefore, mobile operators have sought assistance from the Communications Commission of Kenya (CCK) through the backing of the government to have all mobile users registered using the Kenyan National identity card or a Passport document. Regulators will also need to see evidence that the 'data-richness' of mobile services can serve to protect consumers and mitigate fraud or mis-use.

4.2.2.3 Extortion Messages

The study then sought to know whether there have there been cases of customers receiving extortion messages or ransom messages in a bid to force them to send money to fraudsters unwillingly. The interviewees replied by saying that some subscribers had reported receiving messages from unknown people threatening their lives or the lives of their family members if they did not send money. The same unknown people also send messages claiming to have kidnapped a family member and demanding a ransom to be paid through M-PESA.

In response to this, the company launches investigations once the case has been reported. Aggrieved customers who have lost funds through such means are asked to report to the CID police department who will then work with the company to try and apprehend the offender. As well, mobile numbers that are reported and found to be sending extortion messages are also blacklisted from the market. Subscribers are advised to report the blackmail numbers to the company and to the police department as soon as possible before any funds are sent.

4.2.2.4 Customers Conned to Send Money

The study sought to find out whether there have there been reports of customers being conned to send money using M-PESA by being instructed to do the following on their mobile phone; being guided to the M-PESA send money option unknowingly by the fraudster. The interviewees replied that customers have been conned to send money through a series of tricky steps that are instructed to them which lead them to sending money unknowingly to the fraudster.Being guided to the M-PESA ATM withdrawal option unknowingly and withdrawing funds from the owners account unwillingly. Interviewees indicated that the M-PESA ATM withdrawal option was still a new concept in the menu which a few subscribers were still unfamiliar with. The fraudsters exploit this lack of familiarity with the menu to trick the customers in withdrawing money from their accounts unknowingly. The customer realizes of this deception after receiving a confirmation message from M-PESA.

Being guided to the buy airtime option on the M-PESA menu and then misled to buy airtime for the fraudster's mobile number. The interviewees stated that this fraud trend follows the concept of the send money fraud. Customers are lead to the buy airtime option on the menu through instructions from the fraudster. They are then asked to perform a series of tricky steps that end up in airtime purchase for the fraudster's number. The customer only realizes this deception when they receive a confirmation message from M-PESA.

The study then sought to know the organization's response to the fraudulent activity above. The interviewees responded by saying that the organization has been engaging in aggressive educational campaigns to ensure all subscribers familiarized themselves with the M-PESA menu to avoid confusion leading to loss of funds. These campaigns involve the use of popular television, radio programs and road show campaigns that are tailored to keep the subscribers informed on the new fraud trends and how to report the fraudster's number for investigation. The company also uses normal balance enquiry messages and the official company website (www.safaricom.co.ke) to caution customers against falling victim to fraud. As well, the interactive voice response feature is used to caution customers when they call the customer care helplines.

The company has also invested in acquiring a new simcard that allows subscribers to select the recipient's mobile number before the transaction takes place. This makes it easier for the customer to detect foul play. Quick reporting to the customer care section ensures that money can be recovered through reversal of the customer's funds back to the customer's account before being withdrawn by the offender. Safaricom has also modified the ATM withdrawal option by ensuring a secret pin is required before withdrawal from the ATM and shortening the time within which the authorization code is still viable for withdrawal.

According to Merritt (2010), education and collaboration across organizational jurisdictions and the telecom and financial services industries will be necessary to detect and mitigate criminal activity, fraud, and other payment system risks. Looking to the future, policy and regulation on an international basis will need to consider shared infrastructures that work harmoniously to address emerging risks in retail payments while recognizing the benefits of innovation and increased financial inclusion. Ultimately, mobile money transfer services will demand a paradigm shift in the way retail payment systems are analyzed from a regulatory oversight perspective, first within a country view and then in a cross-border environment.

4.2.2.5 M-PESA Agents and Loss of Funds

The study sought to find out if M-PESA agents reported losing money through customers issuing fake currency while depositing funds into their accounts. The interviewees concurred with these reports stating that some agents had been issued with fake currency after depositing float to a customer's account. The organization to avoid such occurrences trains the agent assistants on how to recognize fake currency and to report to the Police if they come across such a case. The organization encourages the assistant to report to the police as soon as possible so that investigations can be launched.

The study also sought to find out whether agents have had their tills stolen and the float in the tills withdrawn without their consent. The interviewees stated that there have been cases reported though they are few and far between. The interviewees indicated that agents have been cautioned to secure their tills so that unauthorized personnel have no access to it, as well as to keep the secret pin a secret to ensure that the float cannot be withdrawn without prior knowledge. In the cases where those precautions were not followed and the float was indeed withdrawn by unauthorized personnel, the agents are instructed to call the helpline so that the till is barred from further transactions. Agents have been granted their own specific agent help line number to ensure that they are able to receive assistance as quickly as possible.

The study also sought to find out whether agents have been subjected to impersonation of M-PESA staff. The interviewees indicated that some agents have had experiences of some fraudsters coming into the shop masquerading to be Safaricom/M-PESA staff demanding to have access to the tills with sinister motives. These fraudsters have been known to wear and carry Safaricom merchandise which aid to confuse the untrained agent assistants. The organizations response to this has been to retrain the agents on how to recognize the real employees and send numerous communications through pamphlets and text messages to caution the agents against these fraudsters. The information available to the agents about the subscriber has also been limited to absolutely what is required to complete a transaction. This was done after it became evident that fraudsters were using the customer's mobile number indicated on the log book provided to the agents to record transactions to defraud customers who had done deposits. The mobile number is now not recorded which makes it harder for the fraudsters to target users.

The study then sought to find out whether there have been cases reported of customers defrauding agents by giving erroneous details. The interviewees indicated that fraudsters do indeed register using fake identification cards on M-PESA to aid them in acquiring different accounts that disguise their identity making it difficult to apprehend them. The government has made it quite easier for the organization by requiring all mobile users to register their lines using their real identification upon purchasing a Safaricom line which makes it easier to trace the offenders.

The study then sought to find out whether there have been cases reported of agent assistants defrauding their agency. The interviewees stated that the cases reported were also few and far between. The organization urges the agents to vet their employees to ensure they are trustworthy. When such a case has occurred, the agent is to report to the police to facilitate investigations where upon if required, Safaricom will provide law enforcement with necessary requirements to aid in the investigation. Some agents attempt to make more money by defrauding the system. Ploys can include signing up fictitious customers and separating a single deposit into multiple smaller deposits. The organization is continually monitoring agent transactions to ensure that agents do not try to manipulate the commission structure. The organization is swift to respond to agents who are flagged for such activity. The penalties invoked are severe and may lead to the agent being blacklisted from operating or adjustments to the commission structure may be made when a violation occurs.

The management of every organization has to conduct a review that will identify areas of risk. Some actions to consider may include; due diligence on prospective vendors and suppliers and demand controls to avoid unnecessary over ordering of inventory and clear purchasing authorization levels. Previous research done by Cheptumo (2010) has indicated that employee/stakeholders awareness is essential for the effective detection and prevention of fraud.

As such, the company should put in place adequate communication mechanisms for dissemination of information about its fraud and anti-money laundering policy internally and externally.

4.2.2.6 Money Laundering

The interviewees were asked to comment on Safaricom's strategy to combat money laundering. They stated that the organization has an Anti-money laundering policy. It is the policy of Safaricom to prohibit and actively prevent the use of its money transfer services to facilitate money laundering, the funding of terrorist or criminal activity. All employees are encouraged to be conversant with this policy by frequent reminder's using money laundering education through e-mails, quizzes and pamphlets. The organization has also invested in intricate systems designed to flag M-PESA users whose transactions and electronic audit trailsare considered suspicious and may indicate fraudulent trends. The company is continuously improving these systems to accommodate any new trends the fraudsters may use to disguise movement of illegally acquired funds.Employees are also trained to recognize money laundering activity while checking customer accounts and to report any such activity for investigation. When investigations have been done and money laundering activity has been established, the Forensics section in the risk and management division are tasked to work together with law enforcement to apprehend the offending individuals and provide evidence in court if necessary.

In addition, Consult Hyperion (specialists in electronic payments) was commissioned to conduct a second audit of the robustness of the M-PESA platform. They examined the entire M-PESA IT platform with a particular view to ensuring that it could operate safely in the Kenyan market. Most importantly, they checked that all of the M-PESA systems allowed for comprehensive reporting and management so every transaction could be monitored, individually and en masse. This meant that the Central Bank of Kenya could request accurate information regarding the system audit trail, particularly liquidity management, clearing and settlement, and anti-money laundering procedures. The M-PESA platform passed all of the Consult Hyperion's tests for robust operational capacity.

The Central Bank of Kenya policymaking team was comfortable at the conclusion of the review that the system was designed with the Kenyan market in mind (particularly the Anti-Money Laundering systems).

The widely known red flags approach involves the use of a checklist of fraud indicators. The use of red flags is recommended in textbooks on fraud detection and in auditing standards. Red flags increase the possibility of detecting fraud, add structure to the consideration of fraud and provide consistency among auditors. M-PESA transactions are regularly monitored using this approach. However, some have cast doubt on the predictive ability of red flags since they are plagued by two limitations; red flags though associated with fraud, the association may not be perfect and since they focus attention on specific cues, they might inhibit the auditor from identifying other reasons (GSMA, 2008).The use of more sophisticated control systems to flag unusual account activity, based on a customer's user profile, will be needed to detect increasingly complex money laundering schemes.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter is divided into three major sections which are; the summary of the findings, conclusions of the study and discussions of the study based on the objectives of the study.

5.2 Summary of the findings

The study sought to determine the fraud related challenges in the M-PESA service and the strategic responses adopted by Safaricom Limited to address these challenges. The study found that Safaricom Limited was experiencing fraud related challenges in its M-PESA service. There were various types of frauds that had been reported by their subscribers over a period of time. The types of fraud encountered internally by the interviewees include; fraudulent swapping of subscriber lines to obtain funds from the subscribers M-PESA account, sending of start keys fraudulently to enable a fraudster to gain access to the subscribers M-PESA account, soliciting for bribes from potential M-PESA agents to expedite the process of acquiring tills and unauthorized withdrawal of funds from subscribers M-PESA accounts.

The study revealed that a large number of the fraud cases reported were in fact as a result of external influence. The interviewees responded that technology has led to an increase in fraudulent activity because of the surge in the number of mobile phones in the Kenyan market, cheaper airtime and the ease in availability of internet access. The study found that the legal/regulatory environment has been quite helpful in dealing with fraud but indicated that much more needed to be done in combating fraud.

The study also established that hoax text messages, extortion messages, swapping of subscriber lines and customers conned to send money are the most prevalent fraud trends at this moment. M-PESA agents have also been susceptible to falling victim to fraud in various ways which include; being issued with fake currency, stolen tills, agent assistant defrauding agency, M-PESA staff impersonation and identity theft. The study also determined that the company has an anti-money laundering policy that addresses money laundering concerns within the system. The company is continuously improving these systems to accommodate any new trends the fraudsters may use to disguise movement of illegally acquired funds.

The study then found out the strategic responses that the organization has used to deal with past cases of fraudulent activity by employees and to combat fraud within the organization. The study determined that the organization has a fraud policy in place. The management ensures that employees are conversant with the policy by sending regular reminders through e-mails and training sessions for the staff. The interviewees indicated that internal systems and procedures are modified regularly to ensure that the systems are not compromised for fraudulent activity. As well, regular screening of employee activity while using the company's systems is carried out to monitor any ongoing suspicious activity. Avenues to report fraud and whistle blowing have been provided. Training sessions are also held regularly to keep employees informed on fraud risks as well as obtain their participation through feedback on special innovations or procedures to combat fraud. Learning material is also readily available in the form of quizzes, case studies on fraud and printed material such as arm bands and t-shirts that are circulated within the organization to ensure that everyone owns the concept of combating fraud.

The study revealed that a large number of the fraud cases reported were in fact as a result of external influence. The study established that Safaricom works hand in hand with the police CID department to assist subscribers by finding and apprehending perpetrators of fraud crimes. Safaricom has signed a Memorandum of Understanding (MoU) with the Kenya Prisons Service looking to address the mobile phone crime being committed from the confines of the country's prisons. The Communications Commission of Kenya (CCK) has made it easier for the organization to prevent identity theft by requiring all mobile users to register their lines using their real identification upon purchasing a Safaricom line.

The study determined that the organization has dealt with fraud cases by educating the public through mass media communication on all of Safaricom's promotions and the official contact number for winners of these promotions. The organization also places a lot of emphasis on calling their customer care numbers, liaising with the customer care executives through the social media platforms or visiting any of the retail centers to confirm any doubtful information. These campaigns involve the use of popular television and radio programs, normal balance enquiry messages, official company website and interactive voice response features that are tailored to keep the subscribers informed. The newly innovated 3.5K simcard has assisted to combat fraud.

5.3 Conclusions of the Study

The study concludes that fraud is very sensitive and that customers have an immense fear of fraud. The study also concludes that fraud impacts negatively on an organization's reputation. The study found that the organization has a fraud policy in place. The management ensures that employees are conversant with the policy by sending regular reminders through e-mails and training sessions for the staff. The study concludes that Safaricom has encountered instances of customers being defrauded by employees. The types of fraud encountered internally include; fraudulent swapping of subscriber lines to obtain funds from the subscribers M-PESA account, sending of start keys fraudulently to enable a fraudster to gain access to the subscribers M-PESA account, soliciting for bribes from potential M-PESA agents to expedite the process of acquiring tills and unauthorized withdrawal of funds from subscribers M-PESA accounts. The study then concludes that the organization has dealt strategically with these cases by monitoring transactions for any suspicious activity on a regular basis. Employees have also been cautioned against fraudulent activity through the fraud policy. The management has also incorporated a new structure and culture in line with the strategic vision with a view to combating fraud as well as meeting other goals.

The study concludes that technology and legal/regulatory factors have had a huge impact on the rate at which fraud in the mobile sector is growing. The study established that the organization is acquiring the latest technology to aid in curbing fraud. As well, the risk and management division is working hand in hand with law enforcement, prison management and the courts to ensure offenders are punished. The study further concludes that the CCK directive to have all subscribers mobile numbers registered will provide the Operators with valuable identity information deterring further crimes of identity theft. The study also concludes that fraudsters rely heavily on social engineering to acquire customer information that aids them in defrauding M-PESA users. To fight against social engineering the organization embarks on aggressive customer education.

The study also concludes that hoax text messages, extortion messages, swapping of subscriber lines and conned to send money are the most prevalent fraud trends at this moment. The study has established that the organization's primary strategic response has been to educate customers on how to avoid becoming a victim of fraud. Rigorous education campaigns are done through the mass media, social media sites, road show campaigns and through internal appeals for employees to own the concept of combating fraud. Other means of mitigating fraud usually employed by the organization include blacklisting the offender's sim card and mobile phone. Serial offenders are then traced by the organization and apprehended by police where due process of the law is then followed.

The study also concludes that some M-PESA agents have succumbed to fraudster tactics and lost funds. The organization deals closely with the agent networks and law enforcement to ensure that the fraudsters are tracked down and arrested. The study established that agents are also provided with refresher training on new M-PESA services to ensure that they are familiar with all of them. This is done through regular communication with the agent head offices. Any agents who are found to be flouting the policy are served with severe penalties.

The study finally concludes that the organization has anti-money laundering policy. The policy points to the fact that Safaricom aims to prohibit and actively prevent the use of its money transfer services to facilitate money laundering, the funding of terrorist or criminal activity. The organization has also invested in intricate systems designed to flag M-PESA users whose transactions and electronic audit trails are considered suspicious and may indicate fraudulent trends.

The company is continuously improving these systems to accommodate any new trends the fraudsters may use to disguise movement of illegally acquired funds.

5.4 Limitations of the Study

Limitation is an aspect of research that may influence the results negatively, but over which, the researcher has no control (Mugenda and Mugenda 1999). There were only two studies found regarding fraud related challenges in the banking sector. This means that there was no study found regarding fraud related challenges in the mobile money transfer sector with which to make comparisons for the findings in this study.

Some of the respondents did not feel comfortable revealing information that has not yet been cleared to be in the public space. It is for this reason that some of the information that is critical to the strategy on how the company is dealing with fraud has not been included in the findings. It is important that information that gives the organization an advantage over the fraudsters be kept as a company secret.

This study focused on the Mobile Operator's perspective. It would have been of value to obtain views from subscribers and other stakeholders who have been affected directly by fraud. As well, the involvement of other mobile money transfer operators who are plagued by fraud would have helped to give a bigger picture to the prevalence of fraud in the mobile money transfer sector. The study could have been used to find consistency in the strategic responses adopted by these institutions.

5.5 Recommendation for Further Studies

This study has explored the strategic responses adopted by Safaricom Limited in Kenya to address fraud related challenges in the M-PESA service. It has established that fraud is very sensitive and that it impacts negatively on an organization's reputation. The overall effect of fraud can therefore not be ignored at any cost. There is need to do more research and look into other stakeholders perspective such as the customers, suppliers and regulator's role in fraud management.

This study has recommended adoption of various reforms in the M-PESA service and in other arms of the government to reduce fraud related risks in the money transfer services in Kenya. Since technology is changing at a very high rate, another suggestion could be to research the recent technological advances that could further assist in combating fraud.

The study further recommends that another study needs to be done with an aim of investigating the effectiveness of the strategic responses to fraud related challenges in the mobile money transfer sector. This may help to determine whether the findings in this study maybe used by other mobile money transfer operators in combating fraud within their organizations.

5.6 Implications for Policy and Practice

Mobile money merges the regulatory environments of both telecommunications and banking into a new paradigm that ultimately demands a collaborative dialogue to balance intervention for risk mitigation with market innovation. The primary goal of prudential regulation is to protect the interests of consumers and to enhance the integrity of a payment system by ensuring that participants have sound means for identifying, measuring, and managing business risk.

The increased interoperability among shared carrier networks is facilitating data transmission across geographic borders, whereby information about the parties to the mobile money transaction may go undetected by regulators and central banks of customers in the originating or receiving countries. International roaming and the wireless nature of financial transfers may create opportunities for money laundering abuse and other unforeseen financial crimes. The anticipated growth in mobile-enabled remittances requires that regulators contemplate a new environment of international cooperation and sharing of customer data and analysis.

The study recommends that there should be reforms in the police department. This could help to reduce fraudulent activity in every sector. The police are charged with the responsibility of investigating and apprehending criminals. It is the work of the police to carry out thorough investigations in order to penetrate the underworld of fraudsters and thwart fraudulent activity. The study further recommends that since the judiciary is a key player in fraud management, the courts need to be empowered through reforms to hand out more stringent fines and longer jail terms for repeat offenders. The magistrates need to be exposed to international practices in developed countries which have experience in deterring white collar crime and thus understand the gravity of the problem.

Organizations should develop techniques to defend against known social engineering frauds like phishing. Phishing is a technique of fraudulently obtaining private information. The recent surge in smart phone applications may introduce vulnerabilities to malware attacks, which may increase payments risk going forward as bad actors gain access to personal information stored in the handset or accessed through a phone application. Finally, the growing use of SMS as a common technology for sending a payments message may demand further examination of the need to strengthen data encryption.

Mobile operators should establish an arrangement to exchange information on fraud reports which involve their mobile numbers. It has been noted that fraudsters have been using mobile numbers from two different mobile operators which makes it difficult for the operators to trace them or even to prohibit them from continuing to operate as they go about their investigations. A program for routine communication should be established to ensure that all stakeholders are involved in combating fraud.

REFERENCES

Abdalla F. H, Morsheda T. H, Sammy G. A. (1998). *Critical strategic leadership components: an empirical investigation*. Advanced Management Journal: Vol. 63.

Angara, E.O (2010). *Strategic Responses adopted by Kenya Commercial Bank to changes in the environment*. Unpublished MBA project of the University of Nairobi.

Ansoff, H &Mc Donnell, E. (1990) *Implanting Strategic Management*. 2nd Ed. Prentice Hall: Cambridge, UK.

Apostolou, B. (2000a). *Management fraud risk factors*. The CPA Journal pp. 48-52.

Bank Negara Malaysia. (2009). *Policymakers Concur on Need to Harness Technological Advancements to Widen Access to Financial Services*.

Bartlett, B. & Ballantine, D (2002).*The Negative Effects of Money Laundering on Economic Development*. Platypus Magazine, No. 77: Australia.

Chatain, P, Raul H, Kamil B, and Andrew Z.(2008). *"Integrity in Mobile Phone Financial Services:* Working Paper No. 146. World Bank, Washington, D.C.

Chege B.R. (2008) *Competitive Strategies Adopted by Equity Bank Kenya Ltd.* Unpublished MBA project, School of Business, University of Nairobi.

Cheptumo N, K. (2010). *Response strategies to fraud related challenges by Barclays bank in Kenya*. Unpublished MBA project of the University of Nairobi.

Cressey, D. (2007). *Other People's Money*. Patterson Smith: New York

Financial sector deepening Kenya (FSD Kenya).(2009). *Mobile payments in Kenya.* Retrieved from: info@fsdkenya.org

GSM Association (GSMA). (2008c). *"Understanding Financial Regulation and How it Works."* Retrieved from: http://www.gsmworld.com/documents

GSM Association (GSMA). (2007). *Regulatory Framework for Mobile Money Transfers.* Retrieved from: http://www.mobilemoneyexchange.org/Files

Ignacio, M. and Dan R., Bill, Melinda Gates Foundation. (2010). *"Mobile Payments go Viral: M-PESA in Kenya.*" Retrieved from: http://siteresources.worldbank.org/AFRICAEXT/

Ivatury, G. and Mas.I. (2008).*The Early Experience with Branchless Banking.* CGAP Focus.

Johnson, G. & Scholes, K. (2002).*Exploring Corporate Strategy*. New Delhi: Prentice Hall.

Katz, D. (2000). *Elements of a comprehensive security solution*. Pubmed, Vol. 21 pp.12-16.

Kothari, C. (1990). *Research Methodology: Methods and Techniques*. Whira: Prakashan.

Malaysian Approved Standards on Auditing (2001), AI 240 *Fraud and Error*, Malaysian Institute of Accountancy: Kuala Lumpur.

Martin C. (2010) *Strategic responses adopted by Davis & Shirtliff in the changing environment in Kenya.* Unpublished MBA project of the University of Nairobi

Mcguire J. (2003) *Leadership strategies for culture change*. Orlando: Florida.

Merritt C. (2010). *Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments*. Retail Payments Risk Forum. Federal Reserve Bank of Atlanta.

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

Omwansa T. (2009).*M-pesa: Progress and Prospects*. Innovations / Mobile World Congress

Palshikar, G. K. (2002).*The hidden truth, Intelligence Enterprise*.pp.46-51

Pearce, J and Robinson, J. (2005) *Strategic Management: Formulation, Implementation and Control*, 3rd Ed, Irwin Professional Pub.

Porter, M.E. (1985) *Competitive strategy* .Newyork: Free Press.

Safaricom Company Information. (2007). Retrieved from http://www.safaricom.co.ke

Schutt, I. (2007). *The regulatory implications of mobile and financial services convergence*. Vodafone Group Plc

Singh, S. & Shelly, M. (2010).*Review of mobile transfers in the Asia-pacific*. Smart Services: CRC Pty Ltd

Thompson, A., Strickland, A.J and Gamble J.E. (2007). *Strategic Management: Concepts and cases.* 15th Ed, New York: Irwin Inc.

Thompson, J.L. (1997). *Strategic Management: Awareness and Change*. Englewood Cliffs: Prentice Hall.

Thompson, J.L (1994). *Strategic Management: Awareness and Change*. Chapman & Hall, London.

Walliman, N. (2005). *Your research project*. 2ndEd , California: Sage publications

Wanemba, M. (2010).*Strategies applied by commercial banks in Kenya to combat fraud.* Unpublished MBA project of the University of Nairobi.

Wheelhen, T.L & Hunger, J.D. (2008).*Strategic Management and Business Policy.* Prentice Hall. London.

Wishart, N. (2006). *Micro - payment systems and their application to mobile networks:* Infodev

Whitman, D. (1991). *The legal environment of business*. McGraw-Hill Inc.

www.met.police.uk/fraudalert/money_transfer.htm

www.targetmarketingmag.com/article/how-combat-fraud

www.ukfraud.com/money-transfer-scams.html

Yin, R.K (1988).*Case Study Research: Design and Methods*. Newbury Park: Sage Publications

APPENDICES

APPENDIX I: LETTER OF INTRODUCTION TO THE EMPLOYEES OF SAFARICOM LIMITED, M-PESA SECTION

University of Nairobi,
School of Business,
Department of Business Administration,
P.O Box 30197,
Nairobi.

Dear Sir/Madam,

I am a postgraduate student pursuing a Master of Business Administration (MBA) degree at the University of Nairobi. I am carrying out a research on "Strategic responses adopted by Safaricom Ltd in Kenya to address fraud related challenges in the M-PESA service."

Kindly allow me to carry out the study in your organization.

Thanking you in advance.

Damaris Mumbi Ndung'u
M.B.A Student, (UoN).

Prof. Martin Ogutu
Supervisor, (UoN).

APPENDIX II: INTERVIEW GUIDE FOR SAFARICOM LIMITED EMPLOYEES, M-PESA SECTION

Introduction: This interview guide seeks information on Strategic responses employed by Safaricom Limited to fraud related challenges in the M-PESA Service in Kenya. All the information will be treated confidentially and for academic purpose only.

SECTION A

Background information

a) Name of respondent (optional)……………………………………………………

b) Title of the respondent………………………………………………………………

c) Department/Division…………………………………………………………………

d) How many years have you worked for Safaricom Ltd…………………………

SECTION B

1) Is Safaricom experiencing fraud related challenges in its M-PESA service?

   a) Does Safaricom have a fraud policy in place? If so, how does the company ensure that employees are conversant with the fraud policy?

   b) Has Safaricom encountered customers being defrauded by employees in the M-PESA service? If so, what are the types of frauds the organization has had to deal with internally?

   c) Which strategic responses have been applied to deal with past cases of fraudulent activity by employees and to combat fraud within the organization?

2) Does Safaricom experience fraud related challenges as a result of external factors?

   a) Has technology led to an increase in fraud activity in the M-PESA service? If so, how?

   b) In your view, how does the legal/regulatory environment in Kenya impact on fraudulent activity?

   c) How has the organization responded to the factors above?

3) From your experience, do customers receive hoax text messages from persons impersonating Safaricom/M-PESA staff?

   a) Have customers been misled using the hoax messages to send funds unknowingly to fraudsters?

b) How has the company dealt with such cases?

4) Have customers been susceptible to having their lines swapped and funds accessed by unknown people?

a) Does Safaricom have controls in place for assuring recovery of funds lost through fraud? What is the strategic response used to deal with this challenge?

5) Have there been cases of customers receiving extortion messages or ransom messages in a bid to force them to send money to fraudsters unwillingly?

a) What has been the response used by the organization to deal with these reports?

6) Have there been reports of customers being conned to send money using M-PESA by being instructed to do the following on their mobile phone:

a) Being guided to the M-PESA send money option unknowingly by the fraudster?

b) Being guided to the M-PESA ATM withdrawal option unknowingly and withdrawing funds from the owner's account unwillingly?

c) Being guided to the buy airtime option on the M-PESA menu and then misled to buy airtime for the fraudster's mobile number?

d) What is the organization's response to the fraudulent activity above?

7) Have M-PESA agents reported losing funds to fraudsters through the following:

a) Fake currency?

b) Theft of till and access to funds?

c) Impersonation of M-PESA staff?

d) Customers defrauding agents by giving erroneous details?

e) Agent assistant defrauding agency?

f) What are the strategic responses that have been used in dealing with these challenges?

8) What is Safaricom's strategy to curb money laundering?

THANK YOU FOR YOUR TIME AND COOPERATION