

Extent of Credit Card Fraud in the Hotel Industry in Kenya

Yego, Peninah Cheronno

**Submitted in partial fulfillment of the requirements for the Degree of Master of
Commerce at Strathmore University**

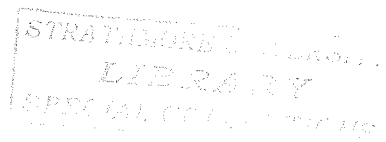
School of Management and Commerce

Strathmore University

Nairobi, Kenya

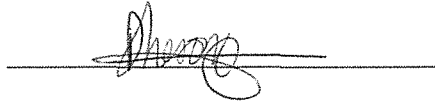
June, 2014

This thesis is available for Library use on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement



DECLARATION

I declare that this thesis is my original work and has not been presented and approved for the award of any degree by this or any other University. To the best of my knowledge and belief, this thesis contains no material previously written or published by another author except where due reference is made in the thesis itself.



Peninah Cherono Yego

3/feb/2015

Date

Approval

This thesis of Peninah Cherono Yego was reviewed and approved by the following:

Dr. David Wang'ombe,

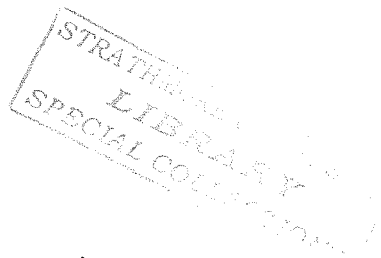
Senior Lecturer, School of Management and Commerce,
Strathmore University

Dr. David Wang'ombe,

Dean, School of Management and Commerce,
Strathmore University

Prof. Ruth Kiraka,

Dean, School of Graduate studies,
Strathmore University



ABSTRACT

This research was conducted with the main objective of establishing the extent of credit card fraud in the Hotel industry in Kenya. The research sought to establish the impact of credit card fraud to this industry, factors that contribute to the fraud and measures that the industry players are taking to address it. The research targeted four and five star hotels in Nairobi, which primarily are target for business and leisure travellers. The empirical study was conducted in a sample of 20 hotels, out of a target population of 25 hotels in Nairobi, Kenya. The target response comprised of the hotel Finance Managers, Information Technology Managers, Credit Control Managers and Internal Auditors.

The research adopted both a descriptive and explanatory research design; data obtained was analyzed using descriptive statistics. The analytical results showed increased acceptance of credit cards as a mode of payments in the hotels. However, fear of fraudulent charges still keeps the clients from using their cards. The respondents placed the financial loss as a result of credit card fraud between Ksh. 0-5 Million annually. It was however seen that fear of damaged hotel reputation is of more concern to the hotels than the financial loss. The study also showed that lost or stolen cards, identity theft, counterfeit credit cards and the internet are common factors that contribute to credit card fraud in hotels. The respondents additionally pointed out hotel cashier's indirect theft from card paying guests as another way through which card fraud occurs in the hotels.

Most respondents indicated that full implementation of the Payment Card Industry Data Security Standards (PCI DSS) was the optimal way for the Hotel industry to mitigate against credit card fraud; this includes ensuring optimal security of client data held or interacted with at the hotels. These measures are already being implemented by some hotels, although still at the initial stages.

STRATHMORE UNIVERSITY
LIBRARY
SPECIAL COLLECTIONS

ACKNOWLEDGEMENT

This research thesis has been a success due to the great support, encouragement and guidance from several people, some of whom I may not mention here, but needless to say that I am forever grateful to.

A very special thanks goes to my family; Mom, Dad, Janet, Lee & Rodgers, Sarah, Kip and Joanne for their encouragement, understanding and support especially during the most challenging times in this journey.

To my friends Joe, Paula, Kigen, Joseph, Mburu, David, Pius, Judy and Florence who contributed in one way or the other in the course of the project and for their constant cheering and support.

I am also grateful to my supervisor, Dr. David Wang'ombe and to Dr. M'cfie for their patience, insights and guidance in ensuring that I successfully delivered this project.

Thank you Almighty God, for your grace every step of the way.

TABLE OF CONTENTS

DECLARATION	i
ABSTRACT	ii
ACKNOWLEDGEMENT	iii
LIST OF TABLES.....	vi
LIST OF ABBREVIATIONS.....	vii
CHAPTER 1.....	1
INTRODUCTION	1
1.1 Background of the Study	1
1.2 Problem Statement	4
1.3 Research Objectives.....	5
1.4 Research Questions.....	6
1.5 Scope of the Study	6
1.6 Justification of the Study	6
CHAPTER 2.....	8
LITERATURE REVIEW	8
2.1 Introduction.....	8
2.2 Occurrence of Credit Card Fraud.....	8
2.3 Impacts of Credit Card Fraud	9
2.3.1 Financial Impacts of Credit Card Fraud	9
2.3.2 Reputational Impacts of Credit Card Fraud.....	10
2.4 Factors Contributing to Credit Card Fraud	11
2.4.1 Credit Card Handling vs. Credit Card Fraud.....	11
2.4.2 Merchant or Card holder Collusion Vs. Credit Card Fraud	15
2.4.3 The Internet vs. Credit Card Fraud.....	16
2.5 Mitigating Measures Against Credit Card Fraud.....	18
2.5.1 Current Developments In Fraud Management in the Credit Card Industry	20
2.6 Theoretical Framework	21
2.7 Gaps in Extant Literature	22

CHAPTER 3.....	24
RESEARCH METHODOLOGY.....	24
3.1 Introduction.....	24
3.2 Research Design.....	24
3.3 Population and Sampling.....	24
3.4 Data and Data Collection.....	25
3.4.1 Data Collection Procedures.....	26
3.4.2 Validity of Instruments.....	26
3.4.3 Reliability of Instruments.....	26
3.5 Data Analysis and Presentation Techniques.....	27
3.6 Ethical Considerations.....	27
 CHAPTER 4.....	 28
RESEARCH FINDINGS	28
4.1 Introduction.....	28
4.2 Response Rate.....	28
4.3 Demographic Information.....	28
4.4 Extent to Which Credit Cards are used to Settle Credit Card Transactions	29
4.5 Analysis of the Impact of Credit Card Fraud in the Hotel Industry.....	31
4.6 Analysis of the Factors Contributing to Credit Card Fraud in the Hotel Industry	33
4.7 Analysis of the Measures Identified to Address Credit Card Fraud in the Hotel Industry.....	36
 CHAPTER 5.....	 40
CONCLUSIONS AND RECOMMENDATIONS	40
5.1 Introduction.....	40
5.2 Discussions	40
5.3 Conclusion	41
5.4 Limitations	42
5.5 Recommendation for Future Research.....	42
REFERENCES	44
APPENDICES.....	49

STRIP
I
FID

LIST OF ABBREVIATIONS

ACFE	The Association of Certified Fraud Examiners
ATM	Automatic Teller Machine
AVS	Address Verification System
BFID	Banking Fraud Investigations Department
CBK	Central Bank of Kenya
CHR	The Centre for Hospitality Research
CVM	Card Verification Methods
FBI	Federal Bureau of Investigation
FS-ISAC	The Financial Services Information Sharing & Analysis Centre
IETF	International Electronic Transaction Facilitators
ISAC	The Information Sharing and Analysis Centre
KAHC	Kenya Association of Hotelkeepers and Caterers
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
UNWTO	United Nations World Tourism Organization
VPAS	Visa Payer Authentication Service

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Credit card fraud has become a significant problem globally (Prabowo, 2012, ACI, 2010). Summers (2011) notes that fraud is inevitable especially for today's consumers, merchants and financial institutions. In her argument, she points out that while in today's world, state of the art detection and prevention mechanisms are in place, the likelihood of being victimized by fraud or a security breach is still alarmingly high, (Summers, 2011). In 2009, Master card and visa card estimated that credit and debit card fraud exceeded US\$10 billion worldwide; financial institutions continue to face an ongoing battle to beat fraudsters in order to protect their customers (MasterCard & Visa, 2009)

According to Bhatla, Prabhu & Dua, (2003), credit card fraud occurs when an individual uses another individual's credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. Accertify (2007) on the other hand examines credit card fraud as an act which may occur with the full knowledge of the card holder, defining it as "friendly fraud". In this case, the card holder or authorized party may use their own credit card to purchase certain goods or services but later dispute the transaction or claim that he or she did not authorize such purchases in the first place.

The effects of credit card fraud have largely been felt by the victims who include card holders, financial institutions and merchants (Baker, D'Amato & Sheridan, 2008). Contrary to popular belief that it is the card holders who are most affected by fraud, Bhatla et al., (2003) observe that it is in fact the merchants who are far more affected by the fraud than card holders. They argue that the consumers' main concern revolves around having the fraudulent charge reversed; merchants on the other hand worry about losses from the cost of the product sold, associated charge back fees, and fear from reputational costs which may include the risk of having their merchant account closed.

Over the years, the number of victims falling prey to credit card fraud has continued to rise just like the volume of losses (ACFE, 2007). As at 2007, statistics from the Association Certified Fraud Examiners (ACFE) in the United States showed that losses arising from credit card fraud had hit \$1 billion (ACFE, 2007), with projections of threefold loss increases. In Indonesia, the Indonesian credit card association placed the magnitude of the losses at \$4.6 million over a period of 3 years to April 2006 (Prabowo, 2012). China is similarly witnessing the effects of credit card fraud, with this type of fraud having been ranked second in the list of economic crimes (Bai & Chen, 2013).

In Kenya, data from the Central Bank of Kenya (CBK) showed that 179,795 credit cards had been issued by November 2013, with credit card transactions totalling to \$22.5million (CBK, November 2013). However, as the level of credit card settlements rise, so too does the losses due to credit card fraud. Shahonya (2014) observes that losses to credit card fraud in Kenya's financial institutions rose to Ksh1.6 billion (\$18.8 million) for the first nine months of 2013, as compared with just Ksh655.6 million (\$7.71 million) reported in the first nine months of 2012. He further adds that as the level of credit card transactions are increasing, criminals are employing more tech-savvy methods of exploiting the credit card systems and are constantly seeking new ways of exploitation (Shahonya, 2014). Ngigi, (2012) notes that International Electronic Transaction Facilitators (IETF) are avoiding the Kenyan market as losses mount from card fraud; Borderlinx, an American company specializing in cross border electronic commerce suspended its operations in the country citing high costs of scrutiny arising from the high incidence of fraud (Ngigi, 2012). The company reported that the fraud largely entailed the use of stolen credit cards to purchase items from online merchants that were destined for Kenyan addresses (Ngigi, 2012).

Research on credit card fraud in Kenya has focused on the banking sector; therefore, statistics of credit card fraud in the banking sectors are readily available, facilitated by the Banking Fraud Investigations Department (BFID), which conducts periodic assessments. Their 2013 report cites credit card fraud as one of the means used to defraud the financial institutions (BFID Report, 2013). According to the Deloitte Financial Crimes Survey Report (2013), credit card fraud contributed 20% of the financial crimes, with recorded

losses of more than \$10M annually. The report focused on the banking, insurance, real estate and capital markets sectors, with 60% of the respondents being drawn from the banking sector (Deloitte, 2013).

The hotel industry in Kenya has continued to witness improved growth both in terms of available bed nights and financially (Kenya Economic Report, 2013). Recently, there has been an up-rise in the number of new entrants joining industry and bringing up new hotels. (Kenya Association of Hotel Keepers & Caterers, 2014). Coupled with the improvements in technology and continued easy availability on internet, making hotel reservations is now easier. However, as seen in cited literature, research on credit card fraud in Kenya places emphasis mostly on the banking and financial services sectors. Hence, statistics on the extent of credit card fraud in the Hotel industry are not available; however, reliance is made on statistics available in the industrialised countries in conducting this research.

Several industries have borne the brunt of credit card fraud in various parts of the world. A study by Trust wave's spider labs (2009) revealed that the hospitality industry was most affected by credit card fraud, more than financial service companies. Their investigation covered 218 data breaches from 24 countries (including United Kingdom, U. S., Germany, Australia, Canada, Hong Kong, Malaysia, Belgium, U.A.E, Switzerland, Saudi Arabia and South Africa). Results of their investigation showed that 38% of the attacks occurred in hotels, 19% occurred on financial services companies, 14.2% on retail stores, 13% on food and beverage industry, 5% on business services, 4% on technology industry, 4% on other industries, 1.4% on the education industry, and 1.4% on the manufacturing industry. The study further revealed that it took an average of 156 days for the businesses to detect the attack once it occurred. (Trust wave's spider labs, 2009).

Credit card fraud occurs in several ways. Bhatla et al., (2003) examines credit card fraud in three broad categories. The first category, fraud related to card handling, comprises of lost or stolen cards, false card application, identify theft, financial fraud and the use of fake and counterfeit cards. The second category comprises of fraud committed through merchants or their employees and that committed by card holders themselves which is

commonly referred to as “friendly fraud”. The third category comprises of fraud committed using the internet. It includes site cloning where fraudsters clone the site of genuine companies from where orders are placed, creating false merchant sites. This involves the use of credit card generators and phishing which is commonly done using emails or instant messaging.

To mitigate some of the fraudulent acts, various mechanisms have been put in place by merchants to prevent further losses including damage to reputation. Bhatla et al., (2003) and Cheney et al. (2012) highlighted some of the technology-assisted credit card detection methods adopted by various players in the industry to deal with the menace. They include the use of network rules, chip and pin cards, neural networks and the use of biometrics. They found that, fraud mitigation is to a large extent coordinated by network rules which must be adhered to by all the players who interact with cards issued by that network. Other measures adopted include the sharing of information related to identity theft and card fraud by both the private and public sector (Cheney et al., 2012).

1.2 Problem Statement

The United Nations World Tourism Organization (UNWTO) identifies Tourism as one of the key pillars of economic growth and as such, it requires key government support world over (UNWTO, 2013). In Kenya, the industry, is one of the key pillars of the economy having contributed an estimate of Ksh. 96.02 billion in revenue earnings to the economy in 2012 (Kenya Economic Report, 2013). This was projected to increase by 2.2 percentage points in 2013 (World Travel and Tourism Council, 2013). In spite of this immense contribution to the economy, the hotel industry, which represents a larger part of the tourism industry, has remained highly susceptible to credit card fraud (Trust wave, 2009). In their study, covering 24 industrialized countries, results of their investigation showed that 38% of the data breaches occurred in hotels. Their study covered the financial services, retail stores, food and beverage, business services, technology, education and manufacturing industries.

There are no statistics to establish the extent of credit card fraud in the hotel industry in Kenya. Studies conducted on the extent of card fraud have largely focused on the

banking, insurance, real estate and capital markets sectors (BFID Report (2013), Deloitte Financial Crimes Survey Report (2013). However, statistics from the Ministry of Tourism show that tourist arrivals in 2012 were 1,780,768. A general overview of these arrivals by region showed that 43% were from Europe, 24% from Africa, 13% from America and 12% from Asia, among other regions (Ministry of Tourism, 2012). As at 30th April 2014, the Ministry had not yet published the 2013 figures. A large population of the U.S. and U.K. market uses credit cards; on average, each person in the U.S. owns 5 cards while in Europe, this figure is at 1.3 cards (Pulina & Paba, 2010). Given this statistic, credit card fraud is most likely to be a problem in the Kenyan hotel industry in future, given that it is a problem in the industrialized countries.

A review of studies by other researches points to a number of gaps. A gap related to the scope of study is evident; most of the studies done so far have examined credit card fraud within the context of financial institutions, mostly banks, insurance, real estate, retail and capital markets sectors. Industries like hotels, which are equally vulnerable, are left out. Prabowo (2012) investigated credit card fraud in Indonesian banks, Deloitte conducted studies on financial crimes in East Africa with a focus on financial institutions in 2013; DelVecchio et al., (2008) focused on consumer perception of risk associated with on-line credit card payments, Bhatla et al., (2003) examined the methods employed by fraudsters, impacts of fraud, prevention and management, while Trustwave's spider labs (2009) investigated the prevalence of credit card fraud in various sectors. This study therefore seeks to fill the existing knowledge gap on credit card fraud in the hotel industry in Kenya by seeking to establish the extent of card fraud, ascertaining the factors contributing to this fraud and measures taken to address the fraud. Information from this study will help strengthen mechanisms of addressing credit card fraud within and outside the hotel industry.

1.3 Research Objectives

1.3.1 Main Objective

The objective of this study is to establish the extent of credit card fraud in the hotel industry in Kenya.

1.3.2 Specific Objectives

The study specifically seeks:

1. To establish the impact of credit card fraud to the hotel industry in Kenya.
2. To establish the factors contributing to credit card fraud in the hotel industry in Kenya.
3. To ascertain the measures put in place to address credit card fraud in the hotel industry in Kenya.

1.4 Research Questions

This study seeks to answer the following questions:

1. How has credit card fraud impacted the hotel industry in Kenya?
2. What factors contribute to credit card fraud in the hotel industry in Kenya?
3. How have the challenges related to credit card fraud in the hotel industry in Kenya been addressed?

1.5 Scope of the Study

This study seeks to establish the extent of credit card fraud in the hotel industry in Kenya. The research establishes the factors that contribute to credit card fraud in the hotel industry in Kenya as well as the measures that have been put in place to mitigate against this fraud. The study focuses on the 4 and 5 star hotels in Nairobi; emphasis is on these hotels as they are most likely to have credit card transactions hence cases of card fraud. The respondents are targeted using an open ended questionnaire. The underlying theory of this research is the Rational Choice Theory, General Deterrence Theory and the Routine Activities Theory.

1.6 Justification of the Study

The study will be of benefit to the hotels players in Kenya. Hotel owners and managers will be better advised on ways of protecting and securing client information, including who has access to this information. The hotels are custodians to numerous client information which may be abused by fraudsters. Hence, this research will help them to be better placed and advised in their decision making concerning data security, network management, web-management and e-commerce management.

Findings from this study will provide beneficial information to government policy makers in the tourism industry and players in the hotel industry who may rely on the research findings in formulating policies and controls to guide usage of credit cards and card security in the hotel industry. Policies and standards on card handling are largely managed by the credit card companies. Government, through the Ministry of Tourism should be involved in policy formulation and standards implementation.

The study will also be important to the Ministry of East African Affairs, Commerce and Tourism, Kenya Association of Hotel-Keepers and Caterers, Kenya Tourism Board and all other tourism players. With this research, they will be able to push for the formulation and implementation of key policies to be implemented by the government, financial institutions and card companies in order to protect their clients and by extension preserve the hotel industry from potential financial and reputational losses.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents a review of literature focusing on the occurrence of credit card fraud and their impacts, factors contributing to credit card fraud, and the measures taken to address such fraud. Key factors under consideration include: credit card handling; merchant or card holder collusion; the internet and mitigating measures. It also reviews theoretical considerations comprising of the Rational Choice theory, the General Deterrence theory, and the Routine Activities Theory.

2.2 Occurrence of Credit Card Fraud

Credit card fraud has evolved with the rapid growth in the credit card industry and has gradually grown to become one of the biggest threats to most business establishments today (Dukhi & Dahake, 2012). According to Bhatla et al., (2003), credit card fraud occurs when one person uses another person's card for personal gain without the knowledge of either the card holder or the card issuer. Additionally, the person using the card may or may not have any relation to the card holder and makes no intention of making it known to him or her that his or her card has been used (Bhatla et al., 2003). It may also occur when a card holder or authorized party uses their own credit card to purchase certain goods or services but later dispute the receipt of the said goods or services or claim that they did not authorize such purchases in the first place (Accertify, 2007).

Bhatla et al., (2003) classified credit card fraud into three categories namely: card related (handling), merchant related, and internet related frauds. Dukhi & Dahake (2012) equally applied the same classification and further observed that fraudsters generally employ different methods in committing fraud. This includes falsification of an application in order to be granted a credit card otherwise known as application fraud; use of lost or stolen credit card; account take-over's and fake and counterfeit cards. Rini (2002) on the other hand classified credit card fraud as being either organized fraud, opportunistic fraud or cardholder fraud. Bhatla et al., (2003) equally observes that card frauds can be

perpetrated through deception (criminal acts), using an account illegally for personal gain, and through account misrepresentation. Sullivan (2010) adds that the processing of credit card transactions largely depends on available information, a factor that draws fraudsters to get this information and use it in perpetrating fraud. This has seen criminals target the computer system, and hence the increase in internet card frauds.

2.3 Impacts of Credit Card Fraud

DeVecchio, Meric, Foltz and Pelletier (2008) in their study to examine how consumers assess the risks associated with online credit card usage observed that consumers generally perceive the risks of settling payments with credit cards as higher than other mode of payments. Results of their study suggested four categories of losses associated with the perceived risk of using credit cards; financial losses, social risks (losses), convenience (time lost) and losses from the failure to detect thefts (DeVecchio et al., 2008). Cheney, Hunt, Jacob, Porter and Summers, (2012) also observe that the actual losses incurred as a consequence of card fraud are wide-spread, and include the actual monetary loss, reputational loss, lost confidence to merchants and private actors and opportunity cost of time spent to verify transactions and replace compromised cards.

2.3.1 Financial Impacts of Credit Card Fraud

Cheney, Hunt, Jacob, Porter & Summers, (2012) opine that credit card fraud is a threat to payment system's efficiency as it degrades operational performance and increases operating costs. They observe that since there are different parties involved in the credit card payment systems' transaction chain, any threat at any point in the chain would cause all parties concerned to incur significant expenses to protect themselves and their clients against fraud. However, it is impossible and inefficient to completely eliminate card fraud, for instance by investing in stronger systems that limit use of stolen cards/card details. Hence, parties concerned must strike a balance between the costs of initiating preventative measures against card fraud and actual costs incurred in the event that they occur in order to maintain efficiency (Cheney et. al, 2012).

Kageyama, (as cited by Pulina & Paba, 2010) documents losses stemming from credit card fraud averaging \$8.2 billion in three years to 2010. This was from a survey of 900

companies at a worldwide level. Kageyama also notes from the survey that card fraud has been on the rise, having registered a 22% increase from the previous year; more firms are now registering existence of card fraud (as cited by Pulina & Paba, 2010).

Verizon's 2012 Data Breach Investigation Report (2012) revealed approximately 855 data breaches in the U.S. as at 2010, which may have compromised up to 5 million card accounts. It has also been observed that companies spend a significant amount of money responding to data breaches. A 2009 survey by Ponemon Institute put this figure at \$200 per client record compromised (Ponemon Institute, 2009). Indirect costs attributed to breached cards is estimated at \$1 billion in the U.S. as at 2010 Cheney et al. (2012).

In recent times, it has been observed that criminals are employing more sophisticated techniques. Criminals are now first intruding into their targets' systems, from where they gather as much information as possible, and then wait for an opportune time to act. When they finally act, the magnitude of the losses is massive, in some cases, the card details are sold to criminal organizations. Cheney et al, (2012) cites an incident in 2008 where a criminal organization instituted a data breach against RBS WorldPay, which resulted in a compromise of numerous prepaid payroll cards. The criminals subsequently used these cards to get \$9 million in cash from ATM's in various cities.

2.3.2 Reputational Impacts of Credit Card Fraud

Besides the financial impact of credit card fraud, another impact witnessed by victims is the reputational impact. Kimani & Thiong'o (2013) note that only a third of all fraud cases are reported, with most financial institutions choosing not to go public out of fear that it could erode their brand name. This observation was based on the Deloitte's Financial Crime Survey 2013 report, which focused on the wider financial services industry across the East Africa region covering Kenya, Uganda and Tanzania with 32 respondents drawn from the banking, insurance, real estate and capital markets sectors (Deloitte, 2013). It is observed that the statistics of financial impacts as a result of credit card fraud are largely understated as victims fear to report incidences due to fear of reputational costs and impacts (Kimani & Thiong'o, 2013). Deloitte's 2013 Financial Crime Survey report showed that while financial institutions across the East African

region were said to have lost in excess of \$30 million in the nine months to September 2013, the figure could have been as high as \$89.41 million since most institutions opt not to report fraud cases (Deloitte, 2013).

Reputation is a key factor in the hotel industry and goes par at par with financial success. A recent study by The Centre for Hospitality Research (CHR) shows that there is an impact of social media on a hotels' financial performance. CHR is an arm of the Cornell University School of Hotel Administration. In their research, they used data from other CHR partners; ReviewPro, STR Global and Travelocity and also relied on other data providers; TripAdvisor and comScore. Their research findings showed that a hotel that puts effort to increase its review scores by 1 point, on a 5 point scale can increase its room rate by 11.2% while still maintaining the same occupancy level. Additionally, a 1% increase in a hotel's on-line reputation leads to a 0.89% increase in its room rate, up to 0.54% increase in its room occupancy and up to 1.42% increase in the average room rate (RevPAR), (CHR, Cornell University, 2012).

Therefore, a hotel that experiences data breach resulting in the compromisation of clients' credit card data in its custody would most likely witness a negative impact in its reputation. This would have resultant effects on its revenues. It has been observed that more clients are consulting TripAdvisor and reading numerous reviews made by other clients and reviewers on the potential hotel of stay, prior to confirming their hotel accommodation bookings (CHR, Cornell University, 2012). TripAdvisor is an online platform that enables independent travellers to share amongst other information, their unbiased hotel reviews and travel experiences from hotels visited; the review also includes price reviews (TripAdvisor, 2013).

2.4 Factors Contributing to Credit Card Fraud

2.4.1 Credit Card Handling vs. Credit Card Fraud

Rice University, (2013) note that since credit card transactions are in essence monetary transactions, they are prone to liquidity risks and hence, they are subject to the same control and reconciliation policies as cash transactions. The university emphasizes that

credit cards should be handled and disposed off in a manner that protects customer information, complies with applicable law, and ultimately complies with the data security standards required by the Payment Card Industry.

Improper handling of card data, whether in electronic or paper form, could lead to a security breach and result in customer ill-will, damages to reputation, fines, legal fees and response-related costs (Rice University, 2013). Each person who has access to credit card information is responsible for protecting that information. Credit and debit card information must be securely destroyed as soon as it is no longer necessary to maintain the information. Physical documents containing debit card information must be stored in secured access-controlled locations such as locked cabinets. The validation code and personal identification number should not be stored in any form. In no case, should credit card information be transmitted via insecure protocols like email or text message (Rice University, 2013). The following types of card frauds occur as a result of poor or improper handling of credit cards:

2.4.1.2 Lost or Stolen Credit Cards

Lost or stolen cards appear to be the most commonly used method of committing fraud. Bhatla et al., (2003) observes this to be the easiest way for fraudsters to get access to card holder information and equally the most challenging form of traditional credit card fraud to deal with. As at 2009, lost or stolen cards contributed to 41% of credit card fraud (Tedder, 2009).

3.4.1.2 Falsification of Card Application

This entails falsification of an application in order to acquire a credit card (Bhatla et al., 2003). It may occur when a person obtains another persons' personal information and uses it to open an account. It may also occur through postal intercepts where a credit card is stolen from a postal service box before it reaches its intended destination. As further observed by Cheney et al. (2012), credit card fraud not only occurs in financial institutions, but also originates from data breaches of client's personal data within custody of the merchants. This information is subsequently used to compromise security controls in financial institutions to commit fraud.

2.4.1.3 Identity Theft

Sproule and Archer, 2007 (as cited in Gilbert & Archer, 2012), defines identity theft as the unauthorized access to an individual's personal information and documents. Identity theft severely manifests itself in card fraud. One common way in which it occurs is when criminals collect numerous clients' personal information which they subsequently use to commit financial fraud, or when stolen cards are used to obtain credit in the victim's name. The criminals mostly operate in organized groups and operate for instance by targeting internet auction sites.

As Pjeloopera and Finklea (2012) observe, identity fraud need not necessarily to take place in the victim's country of residence, this is made possible by online shopping. For instance, in 2010, a Bulgarian national was found guilty of laundering money for a criminal network amounting to \$1.4 million from U.S. victims between 2005 and 2006 (Pjeloopera & Finklea, 2012). Pjeloopera and Finklea (2012) also observe that criminals usually leverage on technological savvy, old-school organized crime strategies, and internet connectivity in executing their frauds. Some criminals go to the extent of placing one of their own employees in the target companies in order to assist them in stealing the credit card details. Cheney et al. (2012), notes that data breaches and identity theft have some influence on consumer payment behaviour. An identity fraud survey report in 2012 showed that over 11 million adults have been victims of identity theft (Javelin Strategy & Research Centre, 2012).

2.4.1.4 Financial Fraud

Another form of fraud related to card handling is financial fraud. It entails provision of false financial information in order to be granted credit (Bhatla et al., 2003). Financial fraud may involve a combination of application fraud, identity fraud and merchant collusion in its execution. In a fraud scam announced by the Federal Bureau of Investigation (FBI) in February 2013, the criminals created more than 7,000 false identities, served as furnishers and thereby providing false favourable information to the credit bureaus regarding credit history of the holders of the false accounts, and in some

cases colluded with merchants of jewellery stores to run the fraudulent cards and split the payments (FBI, February, 2013). The fraudsters stole more than \$200 million.

2.4.1.5 Fake and Counterfeit Cards

Criminals are also generating fake and counterfeit cards and using them to transact (Bhatla et al., 2003). Bhatla et al. (2003) highlights the following methods of creating fake and counterfeit cards:

Erasing the magnetic strip

This entails tampering an existing card that has been acquired illegally by erasing the metallic strip with a powerful electro-magnet. The details on the card are then tampered to match the details of a valid card attained through theft.

Creating a fake card

For a fraudster to be able to create a fake card, they require sophisticated machines as this process requires great effort and skill. However, modern cards have many security features all designed to make it difficult for fraudsters to make good quality forgeries.

Altering card details

Credit card may be altered in numerous ways. One way is to re-emboss them through application of high pressure or heat on the original information embossed in the card by a legitimate card manufacturer. Another way commonly applied by fraudsters is by re-encoding the cards using computer software that encodes the magnetic stripe data on the card.

Skimming

As observed by Bhatla et al. (2003), a large number of counterfeit credit cards involve use of skimming techniques. Skimming involves electronically copying genuine data from a card's magnetic stripe into a fake card. Shahonya, (2014) notes that this method is fast rising as one of the most popular forms of credit card fraud. One of the ways in which skimming takes place in establishments is through the company employees. Employees have been known to be compromised by criminals who issue them with

skimming devices with magnetic stripe readers from which they swipe customer's cards to get hold of their details. Although this method may appear as an old means of harvesting card data, Shahonya, (2014) notes that this technique has undergone mutations such that it poses a danger to the very existence and operation of the magnetic strip cards.

Press (2013), notes that restaurants are most prevalent places where skimming takes place. Ten News.com (2013) notes various skimming methods employed by fraudsters in hotels and restaurants. For instance, waiters have been known to wear skimming devices around their hips, while others are installed at the point of sale on the legitimate stripe reader at the cash register. The skimmed information is then transferred to plastic cards and subsequently used at collusive merchants. The same information can be placed on a magnetic stripe of a lost or stolen card (Press, 2013). This reflects a correlated relationship in the credit card fraud methods.

Another technique employed by fraudsters involves use of high-speed weatherproof cameras mounted around the skimming devices (Press, 2013). A transmitter, which is hooked to the cameras, remits the captured card information to the fraudsters at their location. Press (2013) adds that proper merchant underwriting and monitoring for new merchants can help prevent these frauds. Site visits to merchant locations should also help curb this.

White plastic

A white plastic is a card-size piece of plastic, usually in any colour created by a fraudster. The fraudsters encode this card with legitimate magnetic stripe data and use it for illegal transactions. This card looks like a hotel room key but contains legitimate magnetic stripe data that fraudsters can use at terminals that do not require card validation or verification e.g. petrol pumps and ATMs.

2.4.2 Merchant or Card holder Collusion Vs. Credit Card Fraud

Another observed way through which credit card fraud is perpetrated is through merchant collusion. According to Bhatla et al., (2003), merchant related card frauds are either

initiated by the merchant company or their employees who come into contact with the clients' personal information. Through merchant collusion, merchants may either on their own accord or in collusion with their employee's trade information concerning cardholders' information to fraudsters in return for a payment (Bhatla et al., 2003). The Deloitte Financial Crimes Report, 2013 showed that criminals activities are perpetrated through a combination of internal and external parties collusion which weakens internal controls and creates loopholes for fraud (Deloitte, 2013).

Sim (2000) adds that merchant fraud is multi-faceted. A dishonest merchant may make multiple charges on a client's card and forward them to the clearing house for payment. Merchants have also been known to collude with fraudsters by accepting counterfeit credit cards from which they bill or by selling client's card details to syndicate groups (Sim, 2000).

Card holder collusion to fraud is another way through which credit card fraud is perpetrated. Commonly known as "friendly fraud", this occurs when a card holder disputes a purchase that was authorized by them. In most cases, the card holder uses their own credit card to purchase certain goods or services but disputes the receipt of the said goods or services or claim that they did not authorize such purchases in the first place (Accertify, 2007).

Accertify (2007), further observe that friendly fraud is much a bigger problem in the digital products market because it is much easier for fraudsters to succeed. Merchants always find it difficult to prove that the consumer received the purchased goods or services in a digital setting. Proof of delivery is often difficult and the card holder obtains the goods or services without paying for it.

2.4.3 The Internet vs. Credit Card Fraud

The internet has gradually grown to become a world market bringing together traders from diverse sections of the world to one common market place (Bhatla et al., 2003). Becker, Volinsky, and Wilks (2010) observe that the internet has brought with it more opportunities for fraud. In as much as technology enriches life and creates efficient

operations, it also complicates it and creates a window of vulnerabilities. Sullivan's work affirms this as he observes that criminals' target for information is now directed at electronic records which are largely exhibited through personal information breaches (Sullivan, 2010).

In a bid to accommodate a large pool of merchants and consumers, providers of goods and services are now opening up to electronic payment processing, and in the process opening up an opportunity for fraudsters to gather credit card information (Sullivan, 2010). The target is on getting access to large and sensitive data. Criminals are now getting organized into groups and are even forming underground criminal rackets which then specialize in collecting client data for trade (Sullivan, 2010). For instance, in restaurants, criminals are colluding with the cashiers and waiters and using card readers at the point of sale to gather as much information as possible, which is later used to commit fraud (Sullivan, 2010). This process is called skimming. Poulsen (2009) affirms that this process is gaining prominence and notes that in Florida, skimmed information from restaurants is sold for as much as \$50. Bhatla et al., (2003) describes the following forms of internet credit card fraud:

2.4.3.1 Site Cloning

Site cloning entails fraudsters cloning an entire trading site or just the pages from which a trader is placing his order. The trader will provide card and other personal information on the site, un-known to him that this information is being captured by the fraudster. Given the identical nature of the site with the real site, customers easily fall prey to the site (Bhatla et al., 2003).

2.4.3.2 False Merchant Sites

False credit card sites also work in a similar way with site cloning, as clients are requested to provide certain information in order to access a particular trading site. As Bhatla et al. (2003) explain, the sites usually offer the clients cheap and lucrative services in order to attract mass numbers. In order to access the site, the client is requested to provide all his card details, apparently to be used to verify the client's details as the site service is free.

2.4.3.3 Credit Card Generators

Bhatla et al., (2003) describe credit card generators as computer programs that generate numerous, valid credit card numbers and expiry dates from a single valid account number. The fraudsters use software that works by using the mathematical Luhn algorithm, the same that card issuers use to generate valid card number combinations.

2.4.3.4 Phishing

This entails fraudsters attempting to acquire sensitive information such as credit card numbers, addresses, social security numbers, driver's licence numbers, user names and passwords by appearing as trust worthy organizations in electronic communication. Communication is often done by mail or instant messaging and usually asks clients to provide sensitive information at a website monitored by fraud stars (Accertify, 2007).

2.5 Mitigating Measures Against Credit Card Fraud

In as much as fraudsters are employing sophisticated, technology driven methods to gain access to credit card information and perpetrate fraud, new technologies are equally available to merchants to assist them in detection and prevention of credit card fraudulent activities (Bhatla et al., 2003).

Merchants may employ manual review of credit card transactions for signs of fraudulent activity. Bhatla et al., (2003) however observes that this method requires a high level of human intervention, especially if the transactions are numerous. Hence, this method may prove to be very expensive and time consuming. Another shortcoming also lies in the fact that manual review may not be able to detect some patterns of fraud like use of one credit card in multiple locations (Bhatla et al., 2003).

Another useful technique is the use of Address Verification System (AVS). This technique, mostly used in the card-not-present scenario works by matching the first few digits of the physical address and zip code provided for billing and similar information held by the card issuers. Deviations in this match should raise a red flag.

Card verification methods (CVM) is another technique that may be employed by merchants. As observed by Bhatla et al., (2003), CVM involves use of a 3-4 digit code that is printed and not embossed on the card. This digit is not available on the magnetic stripe. As a control, the merchant may ask the card holder to provide this code, especially for card-not-present transactions. This helps to ensure that the person transacting is in possession of the physical card. This technique however, cannot protect the cardholder and merchant in the event where the card is stolen.

Another control commonly employed by merchants is the creation of a negative list which may be based on such information as client names, addresses, emails, internet protocol (IP) addresses etc (Bhatla et al., 2003). Hence, all payment requests are verified through the negative list and unqualified data is not processed. Master card for example, has a distributed negative list, distributed to merchants and member banks, containing potentially abusive card numbers. Merchants may also use positive lists which are used to recognize trusted clients.

One of the emerging, technology-based controls is the Payer authentication system. This type of service was first implemented by Visa in 2002, called Visa Payer Authentication Service (VPAS). With this service, a client is issued with a Personal Identification Number (PIN) that is associated with the card. This PIN secures a direct authentication channel between the card holder and the issuing bank to facilitate exclusive authorization of online transactions (Bhatla et al., 2003).

Acquiring banks and agents may also adopt lock-out mechanisms that are specifically designed to detect number generator attacks. This is designed to capture cards that have been generated by fraudsters.

Card companies are also on the fore-front in fighting card fraud. Visa and Master card, two of the world largest credit card issuing companies continuously publish a list of merchants who have been found to transact fraudulently in the past. The list maintained by Visa is referred to NMAS while Master Card's is known as MATCH (Bhatla et al.,

2003). This information is particularly important to acquirers when taking on new merchants.

2.5.1 Current Developments In Fraud Management in the Credit Card Industry

Bhatla et al., (2003) observe that technology-assisted credit card fraud detection methods are advancing at a rapid rate. These include network rules, chip and pin cards, neural networks and use of biometrics. Cheney et al., (2012) agree. They observe that currently, fraud mitigation in the credit card industry is to a large extent coordinated by network rules. The rules, established by the networks must be adhered to by all the players who interact with cards issued by that network. The key driver to the networks is the increasing revenues and profitability (Cheney et. al, 2012).

As a result of this, five payment card networks in the card industry private sector; American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc, initially individually established their own data security standards. However, in a bid to better secure the payment card system, they subsequently collectively came together to create a unified set of standards commonly referred to as the Payment Card Industry Data Security Standard (PCI DSS, commonly referred to as PCI). Out of this, the PCI Security Standards Council was born. This council manages the set of data security standards which are expected to be adhered to by all the network participants (PCI, 2013).

Other measures adopted include the sharing of information related to identity theft and card fraud by both the private and public sector. In the U.S. for example, the Information Sharing and Analysis Centre (ISAC) was formed to specifically facilitate information sharing on physical and cyber security threats. Equally, the Financial Services Information Sharing & Analysis Centre (FS-ISAC) was formed. FS-ISAC provides a platform that allows numerous organizations in the public and private sector to share information and alerts related to fraud, cybercrime and data breaches promptly (Cheney et al., 2012).

Lately, most large banks have begun employing fraud mitigation and data security programs in their card payment systems, in a bid safeguard against card fraud. Due to

their size, large financial institutions and merchants may be better placed to implement secure data security systems within their networks as compared to smaller firms (Cheney et. al., 2012).

2.6 Theoretical Framework

There are several theories that exist about crime in general, only recently have experts begun to study cyber crime, on-line crime and credit card fraud within the context of these existing theories (Conradt, 2011). The study entails an examination of the extent of credit card fraud in the hotel industry in Kenya. This is done by establishing the impacts of the fraud, factors that contribute to this fraud and measures taken to mitigate such fraud. The study identified three theories that were applied to further help in understanding the causation and motivation of offenders that engage in credit card fraud.

The Rational Choice Theory states that economic behaviour is generally analyzed using tenets of rational choice (Hayward, 2007). Since credit card fraud is a crime committed primarily for economic gain, rational choice applies when looking at causation and motivation of the offenders. According to the Rational choice theory, offenders are rational people who evaluate the benefits of engaging in a particular criminal behavior against the risks associated with that behavior (McQuade, 2006). In this case, the benefits from engaging in credit card fraud especially those done online are very high and the risks are relatively low. Jurisdictional issues, difficulties in obtaining and preserving evidence, lack of consistency in how laws are applied to cyber crimes by the court, and offender anonymity inhibit apprehension of offenders that offend online (Choi, 2010; Hinduja & Schafer, 2009). In seeking to establish the factors influencing credit card fraud in the hotel industry, this research will seek to find out the extent to which the rational choice theory is of influence. Dukhi & Dahake (2012) and Bhatla et al., (2003) observe that fraudsters generally employ traditional, merchant related ways and the internet in committing card fraud; the study seeks to find out the rationale behind the choice in either of the three methods.

The other theory which the study relates to is the General Deterrence Theory. This theory supports the Rational Choice theory and further adds that in order to deter fraud

offenders, punishment must be swift, certain and severe (McQuade, 2006). Because of the aforementioned reasons, the probability that credit card fraudsters will be caught and face punishment is very low making it difficult to deter this crime which has continued to be on the rise. It has also been argued that in the event such criminals are convicted, the punishment is rarely severe as is the case with most white collar crimes (Boston University, 2012). In establishing the impact of credit card fraud, the study relates this theory to the impacts identified in order to determine whether the lack of swift and severe punishment to offenders contributes the level of impacts of credit fraud that are established.

The study also applies the Routine Activities Theory which puts forth that crimes happen when motivated offenders come in contact with suitable targets under a lack of capable guardianship (McQuade, 2006). The following factors according to Routine Activities Theory increase the risk of victimization: exposure to offenders, deviant behaviour, and target attractiveness. The presence of guardianship acts as a protective factor (Spano and Frielich, 2009). According to this theory, motivators of online credit card fraud are drawn to online sites because of the presence of attractive targets (customers) who are willing to purchase high cost items online, irrespective of their geographical location. The lack of proper guardianship in online sites further compounds the problem as people are allowed to create accounts without thorough background checks. Most victims increase their exposure to fraud the more frequently they buy things through online sites (Boston University, 2012). In seeking to establish measures taken by the hotels to address the extent of credit card fraud, the research relies on this theory and seeks to find out if the hotels have put in place any measures to deter potential fraudsters who would want to access client data in the hotels' possession. This research therefore adopts all the three aforementioned theories in meeting the three research objectives.

2.7 Gaps in Extant Literature

This chapter covered literature on the occurrence of credit cards; the relationship between credit card handling and credit card fraud, the relationship between merchant or card holder collusion and credit card fraud; the relationship between the internet and credit card fraud; mitigating factors and current trends in fraud management. From the

literature, it is evident that the way credit cards are handled by either the card holders or the merchants determine to a greater extent whether credit card fraud will be committed or not. Likewise, merchants and their employees just like card holders and their representatives may collude and abet credit card fraud. It is also discernable that the internet opens up various platforms through which credit fraud can occur. From the literature, we can also observe that in as much as the techniques adopted by fraudsters in employing card fraud have evolved to keep pace with the changing technology, the forms of technology-assisted credit card fraud detection methods are advancing at a rapid rate. However, the literature reviewed is not specific to the hotel industry, aside from the factors indicated as contributing to card fraud, the researchers have not mentioned specific factors that are attributed to credit card fraud in the hotel industry. This is important in establishing specific measures that can be implemented to counter credit card fraud in the hotel industry. The literature reviewed also cited the impacts of credit card fraud and notes two main impacts; financial and reputation. However, the financial impact to the hotel industry is not stated. Literature reviewed has generally stated financial impacts to the banking, financial services, retail and insurance sectors. The tourism industry being a key pillar of the economy, it is equally important the impact of card fraud to this industry is determined. The literature also reviewed various theories that exist around credit card fraud to further help put the study into context. From the theories, we can attribute credit card fraud to economic drive, self belief due to routine, lack of proper guardianship and lack of adequate deterrent measures. This chapter also outlined the relationship between the dependent and the independent variables of the study.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This research aims at establishing the extent of credit card fraud in the Hotel industry in Kenya by establishing the impact of credit card fraud, factors contributing to this fraud and measures taken to address this. The Rational Choice Theory, General Deterrence Theory and Routine Activities Theory are applied. This chapter presents the methodology that was used to conduct the study. The study sets off by presenting the research design, location of the study, population, sampling procedure, sample size, data collection instruments and data analysis procedures that are used in the study.

3.2 Research Design

The research was both descriptive and explanatory in nature. It was descriptive as it sought to describe the characteristics of the target population by providing summaries concerning the sample studied describing the data and observations made on the sample. The research was explanatory as it sought to establish the impact of credit card fraud in hotel industry in Kenya and analyse the factors that contribute to credit card fraud in the hotel industry in Kenya as well as the measures that have been put in place to mitigate the fraud. Given (2008) notes that explanatory research posits that the research in question is intended to explain, rather than simply to describe, the phenomenon studied.

3.3 Population and Sampling

Cox, (2008) describes a target population as the entire set of units for which the survey data are to be used to make inferences. Hence, the target population describes those units for which the findings of the survey are meant to generalize (Cox, 2008). The target population of the research consisted of all the 4 star and 5 star rated hotels in Nairobi, making up a total of 25 hotels. The Ministry of Tourism is mandated to rank all hotels based on a pre-determined criteria. This ranking was last done in 2003 via gazette notice (*Appendix 1*). Since then, there has been an uprising of new hotels in the market. Therefore, the list of target hotels was based on the Ministry's last ranking and the ranking by the Kenya Association of Hotelkeepers and Caterers (KAHC), based on its

member listing. The researcher considered this target population as these hotels are mostly business and tourist hotels and are more likely to have transactions carried out by credit cards. According to the KAHC members listing, a majority of the four and five star hotels operate in Nairobi, for this reason, the population and sampling was focused on Nairobi hotels as they are representative of the Kenyan environment. A list of all the 4 and 5 star hotels in Nairobi can be found in *Appendix 2*.

The researcher used both purposive and random sampling to determine the target respondents of 20 hotels. Purposive sampling was first used to choose four and five star hotels as the four and five star hotels are largely business and tourist hotels which attracts the high end clientele who are most likely to use credit cards due to their high spending. Out of the 25 hotels in the population, 13 were five star and were all selected. Random sampling was then used to choose 7 four star hotels; all the four star hotels in the population were adequate to provide the necessary information for the research given their description in the KAHC member listing. A total of 20 target hotels was therefore selected. *Appendix 3* contains all the 20 the target hotels.

The target respondents comprised of four respondents from each of the hotels sampled. The target respondents consisted of the Finance/Credit Managers, Front Office Managers, Information Technology Managers and Internal Auditors. This target was selected since this represented the pool of people who interact with credit card transactions and decision making in the hotel and would be aware of any challenges associated with credit cards. 80 respondents were targeted.

3.4 Data and Data Collection

The research sought to collect data to establish the extent of credit card fraud in the select hotels and data to indicate other impacts of credit card fraud in the hotels. This was to enable the determination of the impact of credit card fraud in the hotel industry. Data was also sought to establish the factors affecting credit card fraud in order to establish how the fraud occurs in the hotels and what factors foster this fraud. The research also sought to find out data to establish measures taken by the hotels to mitigate against credit card fraud in the hotels. Semi-structured questionnaires were used to collect data from the

respondents. This method is preferred because it gives a wide range of options to the respondents. The questionnaires were designed to enable the respondent respond on a five point scale, while some questions were open ended. The questionnaire can be found in *Appendix 4*.

3.4.1 Data Collection Procedures

The researcher visited the selected hotels and explained to the management the purpose of the study and what the study entailed. During the visit, the researcher provided the hotel management a letter of permission from the University as proof that indeed the research is for study purposes. A copy is filed in *Appendix 5*. The researcher then administered the questionnaires to respondents giving them a period of five days to allow for sufficient time to accurately respond to the questions. Questionnaires were then collected from the respondents thereafter.

3.4.2 Validity of Instruments

Validity of data instruments refers to the accuracy or meaningfulness and technical soundness of the research. It is the extent to which a test measures what it was intended to measure (Mason, et al, 1989). To ensure validity of research instruments, the researcher conducted a pilot study targeting five (5) respondents from hotels which were not sampled. These respondents were excluded from the main study. The pilot sought to establish whether the instruments measured what they intended to measure, whether they represented the content, their appropriateness to the sample or population and whether they were comprehensive enough to collect all the information needed. Feedback from the pilot informed adjustments that were made on the instruments.

3.4.3 Reliability of Instruments

Reliability of a research instrument relates to the extent to which the instrument yields the same results on repeated trials (Carmines & Zeller, 1991). To ensure reliability of research instruments, a pilot test was carried out on five (5) respondents from hotels which were not sampled. These respondents were excluded from the main study.

3.5 Data Analysis and Presentation Techniques

Both qualitative and quantitative data was collected from the study. Raw data was edited both at the field and centrally to ensure that the data was accurate, consistent with other information, uniformly entered, complete and arranged to simplify coding. Responses obtained were categorized into themes around the independent and dependent variables. Coding was done manually in a code sheet and the results entered into the SPSS system which was used to present results in form of frequencies and percentages, outlined in frequency tables. Cross tabulations was used to examine frequencies of observations belonging to specific categories on more than one variable. The extent of credit card fraud and factors contributing to credit card fraud in the Hotels under study were therefore measured and presented using frequencies and percentages

In order to establish the measures put in place to address the problem of credit card fraud in the hotels, data collected was also analysed through content analysis. According to Hancock (2002) this involves "a procedure for the categorization of verbal or behavioural data, for purposes of classification, summarisation and tabulation.' Due to the qualitative nature of the data collected to address objective 1 and 3 the researcher used content analysis.

Hancock (2002) notes that the content can be analyzed on two levels: basic and higher level. The researcher used the higher level of content analysis in order to offer an in depth analysis of the data collected and to develop meaningful recommendations and draw accurate conclusions.

3.6 Ethical Considerations

The researcher conducted the research process ethically. Care was taken to ensure minimal disruption of the respondent's duties at their place of work. The respondents were adequately briefed on the purpose of the study, objectives and respondents participation. The researcher assured the respondents of confidentiality to all information received.

CHAPTER 4

RESEARCH FINDINGS

4.1 Introduction

The research findings are presented in this chapter. First, an analysis of the respondents is done, by looking at the response rate and the demographics of the respondents. An analysis of the responses to each variable is then reviewed, placing an emphasis on the objectives of the study. Descriptive statistics was generally used in reviewing the pattern of data collected in relation to each variable. This is done in the form of frequency tables, percentages and mean scores. The data collected was summarized in Microsoft Excel and analysis done using statistical package for social scientists (SPSS V. 16).

4.2 Response Rate

The research targeted 20, Four and Five star hotels in Nairobi with at least 4 respondents targeted in each hotel, making up an expected 80 respondents. A total of 39 respondents responded from all the 20 hotels sampled making up 49% response rate. There were responses from each of the hotels targeted although none of the hotels had responses from the expected 4 respondents. The response rate was low as the hotels have different people who handle credit card related transactions and the respondents varied from hotel to hotel. Not all the 4 targeted respondents consistently handled credit cards in the sampled hotels.

4.3 Demographic Information

The first section of the questionnaire presented to the respondents sought to gather general information from the respondents with the objective of establishing whether the respondents bore sufficient experience and knowledge in the hotel industry to sufficiently provide the information needed in order to adequately address the research objectives. The results were analyzed and resented in frequencies and percentages, as detailed in table 4.1 below.

A majority of the respondents, 51%, were from the Finance department and worked as Finance Directors, Finance Managers or Credit Control Managers. 20% were IT

Managers, while 15% and 12% were Internal Auditors and Front Office Managers respectively. A majority of the respondents, 61%, indicated that they had worked in the hotel industry for between 6-15 years. 20% had over 16 years in the hotel industry while 17.9% had less than 5 years' experience in the industry. Therefore, the respondents had adequate experience in the hotel industry to provide data for this research analysis.

Table 4.1: General Research Demographic Information

Variables		Frequency	Percent	Cumulative Percent
Department	Position/ Job Title			
Administration & General	Internal Auditors	6	15.4	15.4
Finance	Finance Directors/ Managers/ Credit Managers	20	51.3	66.7
Front Office	Front Office Managers	5	12.8	79.5
Information Technology	Information Technology Managers	8	20.5	100
Total		39	100	
Years of Experience	0-5 years	7	17.9	17.9
	6-10years	10	25.6	43.6
	11-15years	14	35.9	79.5
	16-20years	8	20.5	100
	Total	39	100	

4.4 Extent to Which Credit Cards are used to Settle Credit Card Transactions

In order to establish the impact of credit card fraud in the hotel industry, which was the first objective, the research sought to find out the extent to which credit cards are used to settle transactions in the hotels under study. A five point scale was used to determine the respondents' perception on the extent of use. The responses as summarized in table 4.2 below showed a significant use of credit cards in the hotels as a mode of payment. 43% of the respondents said that credit cards were used by guests to settle bills to a great extent, while 51% stated that this was most commonly used. Only 5% said that this is commonly used.

Table 4.2: Extent of use of Credit Cards to Settle Transactions

Variables		Frequency	Percent	Cumulative Percent
Extent of Credit Card Use	Commonly Used	2	5.1	5.1
	Most Commonly Used	20	51.3	56.4
	Used to a Great Extent	17	43.6	100
	Total	39	100	

The research further sought to find out factors that encourage the use or lack of use of credit cards as a mode of payment. 10 variables were identified from academic literature that influences the use of credit cards. The respondents were asked to rank each factor on a five point scale stating their agreement or disagreement. The results, as detailed in table 4.3 below, showed that respondents highly ranked the following factors; increased acceptance of credit cards as a mode of payment, easy availability of credit, increased internet/ on-line transactions and secure credit card platforms as contributing to the level of use of credit cards in hotels. The respondents did not feel that decreased ability to save encourages use of credit cards in the hotels.

Table 4.3: Factors Contributing to Acceptance of Credit Cards as a mode of Payment

Variable	Mean	Ranking Scale	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Easy Availability of Credit	3.8	Frequency	2	2	7	16	12	39
		Percentage	5.1	5.1	17.9	41.0	30.8	100
Increased Acceptance of C/Card as a Mode of Payment	4.38	Frequency	1	0	2	16	20	39
		Percentage	2.6	0.0	5.1	41.0	51.3	100
Increased On-line/Internet Transactions	3.58	Frequency	4	3	8	14	10	39
		Percentage	10.3	7.7	20.5	35.9	25.6	100
Decreased Ability to Save	2	Frequency	12	19	6	1	1	39
		Percentage	30.8	48.7	15.4	2.6	2.6	100
Secure Credit Card Platforms	3.39	Frequency	1	4	16	15	3	39
		Percentage	2.6	10.3	41.0	38.5	7.7	100

The respondents equally ranked the following variables identified as contributing to non-acceptance of credit cards as a mode of payment. The respondents pointed out that fear of exposure to credit card fraud and insecure swiping platforms contribute more to non-

acceptance of credit cards as a mode of payment. The results are presented in table 4.4 below.

Table 4.4: Factors Contributing to Lack of Acceptance of Credit Cards as a mode of Payment

Variable	Mean	Ranking Scale	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Fear of Exposure to Fraud	3.21	Frequency	3	9	9	10	6	37
		Percentage	8.1	24.3	24.3	27.0	16.2	100
Non-Acceptance of C/cards as a Mode of Payment	2.16	Frequency	12	12	9	3	1	37
		Percentage	32.4	32.4	24.3	8.1	2.7	100
Insecure Swiping Platforms	2.54	Frequency	7	12	10	7	1	37
		Percentage	18.9	32.4	27.0	18.9	2.7	100
Market Preference for Debit Cards	2.16	Frequency	11	12	11	3	0	37
		Percentage	29.7	32.4	29.7	8.1	0.0	100
Desire for Simple Lifestyle	2.41	Frequency	12	11	6	3	5	37
		Percentage	32.4	29.7	16.2	8.1	13.5	100

4.5 Analysis of the Impact of Credit Card Fraud in the Hotel Industry

In order to address the first objective on the impact of credit card fraud in the hotel industry, the respondents were asked to state if they had witnessed credit card fraud in their hotels. 100% of the respondents affirmed that they had witnessed credit card fraud in the hotels they work for. The results are detailed in table 4.5. The respondents were then asked to indicate the magnitude of fraudulent credit card transactions in their hotels. 53.8% of the respondents placed the magnitude of fraudulent card transactions in their hotels at less than 5% while 43.5% placed this at 5-10%. Only 2.6% placed this magnitude at between 10-20%. This result is detailed in table 4.6 below.

Table 4.5: Incidences of Credit Card Fraud

Variables	Response	Frequency	Percent	Cumulative Percent
Incidence of Credit Card Fraud	Yes	39	100	100
	No	0	0	

Table 4.6: Magnitude of Fraudulent Credit Card Transactions in the Hotels

Variable	Magnitude of Credit Card Transactions		
	Frequency	Percent	Cumulative Percent
0-5%	21	53.8	53.8
5-10%	17	43.6	97.4
10-20%	1	2.6	100
Over 20%	0	0	
Total	39	100	

The summary of literature reviewed pointed out two main impacts of credit card fraud namely financial and reputational impacts (Pulina & Paba, 2010, Cheney et al., 2012, Deloitte, 2013, CHR Cornell University, 2012 etc). In seeking to find out the extent of financial impact of credit card fraud in the hotels sampled, the respondents were then asked to indicate an estimate of the annual financial losses incurred by the hotel due to credit card fraud. Given that 95% of the hotels sampled are private companies not listed in the stock exchange, the respondents were only asked to provide an estimate from a range provided in order to discourage non-response. Test results are as presented in table 4.7. The questionnaire did not ask the respondents whether they felt that reputational risk was another impact of credit card fraud in their hotels. In order to further address this objective, the respondents were instead asked to indicate other impacts of credit card fraud in their hotels. The results are presented in table 4.8.

Table 4.7: Annual Estimated Financial Losses from Credit Card Fraud

Range in Ksh.	Annual Estimated Financial Loss		
	Frequency	Percent	Cumulative Percent
0-2 Million	27	69.2	69.2
2.1 Million-5 Million	9	23.1	92.3
5.1 Million-10 Million	0	0	92.3
Above 10 Million	3	7.7	100
Total	39	100	

Table 4.8: Non-Financial Impacts of Credit Card Fraud to the Hotel Industry

Variable	Annual Estimated Financial Loss		
	Frequency	Percent	Cumulative Percent
Hotel reputation	29	93.5	93.5
Clients fear to use credit cards	2	6.5	100
Total	31	100	

Results of the research showed that financial losses from credit card fraud is estimated at below Ksh. 2 million annually in 69% of the hotels sampled. 23% of the respondents placed this loss at between Ksh. 2.1 million and Ksh. 5 million while only 7.7% of the respondents placed it at above Ksh. 10 million annually. While these results may portray an insignificant level of credit card fraud in the hotels sampled, the research findings showed significant reputational impacts of credit card fraud to the hotels. 93% of the respondents stated reputational impact as the other impact of card fraud in their hotels, when asked to indicate other impacts of card fraud to their hotels. Only 6.5% mentioned client's fear to use credit cards as a mode of payment.

The results for this objective conform to the literature reviewed as seen in other research findings. Kimani & Thiong'o (2013) noted that only a third of all fraud cases are reported, with most financial institutions choosing not to go public out of fear that it could erode their brand name. This observation was arrived at based on a survey conducted in the financial services industry across the East Africa region covering Kenya, Uganda and Tanzania with 32 respondents drawn from the banking, insurance, real estate and capital markets sectors (Deloitte, 2013). Hence, findings of this research are not far from the findings in the financial services sector. Reputational risk is a key impact to the hotel industry much more than the risk of financial losses. The Centre for Hospitality Research (CHR) also linked lost hotel reputation to the long term financial loss to the hotels. In their research, they demonstrated that lost hotel reputation due to bad publicity ultimately leads to reduced hotel revenues due to reduced occupancies which force the hotels to reduce their room rates (CHR Cornell University, 2012). A hotel guest who experiences credit card fraud may tarnish the hotels' reputation for instance on hotel review sites like TripAdvisor.

4.6 Analysis of the Factors Contributing to Credit Card Fraud in the Hotel Industry

The second objective of the research was to identify the factors that contribute to credit card fraud in the hotel industry. Academic literature broadly classifies these factors in to three; card related (card-handling), merchant related, and internet related frauds (Bhatla et al., 2003, Dukhi & Dahake 2012, etc). The questionnaire provided to the respondents

listed down variables identified in literature and classified under the three categories. The respondents were asked to rank them using a five point scale. The results of the test, was analyzed using frequencies, percentages and mean statistics, as presented in table 4.9 below.

Table 4.9: Factors Contributing to Credit Card Fraud in the Hotel Industry

Variable	Mean	Ranking Scale	Rare	Slightly	Common	Most Common	Extremely Common	Total
Lost/Stolen Cards	2.92	Frequency	6	8	12	9	4	39
		Percentage	15.4	20.5	30.8	23.1	10.3	100
Identity Theft	2.90	Frequency	2	12	14	10	1	39
		Percentage	5.1	30.8	35.9	25.6	2.6	100
Counterfeit Credit Cards	2.56	Frequency	7	12	12	7	1	39
		Percentage	17.9	30.8	30.8	17.9	2.6	100
Falsification of Financial Information	2.03	Frequency	15	13	6	5	0	39
		Percentage	38.5	33.3	15.4	12.8	0	100
Employee Collusion with Fraudsters	1.95	Frequency	14	17	5	2	1	39
		Percentage	35.9	43.6	12.8	5.1	2.6	100
Customer Collusion with Fraudsters	1.92	Frequency	18	11	6	3	1	39
		Percentage	46.2	28.2	15.4	7.7	2.6	100
Internet/E-commerce Activities	3.03	Frequency	6	10	7	9	7	39
		Percentage	15.4	25.6	17.9	23.1	17.9	100
Site Cloning	1.69	Frequency	20	14	3	1	1	39
		Percentage	51.3	35.9	7.7	2.6	2.6	100
Phishing	2.18	Frequency	14	13	5	5	2	39
		Percentage	35.9	33.3	12.8	12.8	5.1	100

Overall, the research findings showed that internet and E-commerce activities, lost or stolen credit cards and identity theft are the factors that are most applied in perpetrating credit card fraud in the hotels, with means of 3.03, 2.92 and 2.90 respectively. The N factor for the mean calculation was 39 with a minimum value of 1 and a maximum value of 5. These results are in support of the findings by other researchers as seen in the literature reviewed.

Literature reviewed showed that tech-savvy criminals are always constantly finding new ways to exploit the credit card systems (Shahonya, 2014). Sullivan's work affirmed this, he observed that criminals' target for information is now directed at electronic records which are largely exhibited through personal information breaches (Sullivan, 2010). The research findings affirmed this literature; 17.9% of the respondent stated that credit card fraud perpetrated through the internet and other e-commerce sales was extremely common; 23% said this was most common while 17.9% stated that this was common. Overall, this means that 59% of the respondents highly attributed credit card fraud incidences in their hotels to internet-related factors. However, it was interesting to note that the respondents did not think that site cloning and phishing, which are forms of internet credit card fraud factors (Bhatla et al., 2003) are common. 51% of the respondents opined that site cloning was a rare occurrence in the hotels, while 35.9% said that phishing was a rare occurrence.

10% of the respondents were of the opinion that lost or stolen cards were extremely used to perpetrate card fraud, 23% felt that use of this method was most common while 30% felt that this was common. 30% of the respondents felt that identity theft slightly contributed to card fraud while 35% and 25% opined that identity theft was common and most common respectively. This finding supports observations by Kimani & Thiong'o (2013); they noted that the BFID 2013 reports listed identity theft as among the most common ways used to defraud financial institutions.

The respondents also stated minimal cases of counterfeit credit cards, employee/customer collusion with fraudsters and falsified financial information used to facilitate credit card fraud. Cases have been identified in literature where clients falsify their financial information in order to obtain credit cards which they subsequently use, resulting in losses to the persons who accept them (Bhatla et al., 2003). 38% of the respondents were of the opinion that this was a rare occurrence in the hotels while 33% stated that they had witnessed slight cases. Employee and customer collusion with fraudsters is another way through which credit card fraud is perpetrated. Majority of the respondents did not feel that card fraud occurs through this means in the hotels. Only 7.7% of the respondents opined that employee-fraudster collusion in the hotels was most

and extremely common while only 10% of the respondents felt that customer-fraudster collusion was most and extremely common. 30% of the respondents felt that counterfeit credit cards were slightly and commonly used to perpetrate card fraud while 17% felt that this was both rare and most common.

4.6.1 Other Factors Contributing to Credit Card Fraud in the Hotel Industry

The research sought to find out from the respondents other factors that contribute to credit card fraud, specific to the hotel. Open ended responses were obtained and each mentioned variable coded and tabulated as presented below. As seen in the responses presented in table 4.10 below, 72% of the respondents stated other ways in which credit card fraud occurs in the hotel is through employee indirect theft from guests. This mostly occurs when employees amend the mode of payment for cash paying clients and route the bills settled to accounts of card paying clients.

Table 4.10: Other Factors Contributing to Credit Card Fraud in the Hotels

Variable	Other Factors Contributing to Card Fraud		
	Frequency	Percent	Cumulative Percent
Hotel staff, mostly cashiers, who route bills settled by cash to a client settling via credit card and pockets the cash.	18	72	72
Numerous internet related threats	2	8	80
Counterfeit credit cards e. g 'Card not present'	3	12	92
Forged third party authorization forms	1	4	96
Hotel employee negligence e. g lack of proper verification of card holder identity and signature	1	4	100
Total	25	100	100

4.7 Analysis of the Measures Identified to Address Credit Card Fraud in the Hotel Industry

The literature reviewed identified wide-spread measures taken by different industry players to address credit card fraud in varied industries. However, since the measures were not specific to the hotels, six specific measures to the hotel industry were identified during the pilot study. The respondents were provided with these measures and asked to

rank their adoption in their hotels on a 5-point scale. The test results for this objective are detailed in table 4.11 below.

The results were analyzed using frequencies, percentages and mean statistics. Overall, it was observed that the hotels have adopted all the six measures in their hotels to address credit card fraud. The mean differential between the most and least ranked variable was 0.85, this was based on a minimum scale of 1 and a maximum of 5, and an N value of 38. The most ranked variable, stringent password policy had a mean of 4.4 while the least ranked, segregation of duties & role separation had a mean of 3.55. This implies that all variables identified are important in addressing credit card fraud in the hotel industry. However, 10% of the respondents felt that segregation of duties and role separation was not adequate in addressing card fraud.

Table 4.11: Identified Measures to Address Credit Card Fraud in the Hotel Industry

Variable	Mean	Ranking Scale	Least Adopted	Slightly Adopted	Commonly Adopted	Most Adopted	Extremely Adopted	Total
Implementation of Payment Card Industry Data Security Standards	3.79	Frequency	2	3	7	16	11	38
		Percentage	5.2	7.8	15.8	42.1	28.9	100
System Interfacing (Front Office & Back Office)	4.16	Frequency	0	3	5	13	17	38
		Percentage	0	7.9	13.2	34.2	44.7	100
Stringent Password Policy	4.40	Frequency	1	1	2	11	22	37
		Percentage	2.7	2.7	5.4	29.7	59.5	100
Stringent Controls for On-line Bookings	4.21	Frequency	0	2	5	14	17	38
		Percentage	0	5.3	13.2	36.8	44.7	100
Continuous Staff Training	4.37	Frequency	0	2	2	14	20	38
		Percentage	0	5.3	5.3	36.8	52.6	100
Segregation of Duties & Role Separation	3.55	Frequency	4	3	7	16	8	38
		Percentage	10.5	7.9	18.4	42.1	21.1	100

4.7.1 Suggestions on the Measures to be taken to Address the Problem of Credit Card Fraud in the Hotel Industry in Kenya

Aside from the specific measures taken to alleviate credit card fraud in the hotels under study, the respondents were asked to state measures that the Hotel Industry in Kenya can take to address this problem. The measures listed below were highlighted and their frequencies summarized in table 4.12 below. Overall, 31.7% of the respondents stated that full implementation of the Payment Card Industry Data Security Standards (PCI DSS) is key in addressing card fraud. 23.8% placed emphasis on employee training and sensitization while 20.6% mentioned information security, which is one of the components of PCI-DSS.

These findings support the findings on current developments in fraud management in the credit card industry. Cheney et al., (2012) observed that currently, fraud mitigation in the credit card industry is to a large extent coordinated by network rules, which must be adhered to by all the players who interact with cards issued by that network. The PCI DSS guidelines were established by EMV, and are managed under the PCI Security Standards Council, which should ensure adherence by all network participants (PCI, 2013). A way in which the hotels have adopted these rules is in the implementation of the chip and pin cards, which assures the guest of a secure swiping platform. Hotels are also protecting client data in their possession for instance through masking of card numbers.

Table 4.12: Suggested Measures to Address Credit Card Fraud in the Hotel Industry in Kenya

Variables	Frequency	%	Cumulative %
Information sharing by hotels on fraud methods and details of known fraudsters	3	4.8	4.8
Information security e. g data encryption during transmission, truncation of card numbers	13	20.6	25.4
Full implementation of the Payment Card Industry Data Security Standards (PCI DSS)	20	31.7	57.1
Employee training and sensitization	15	23.8	81.0
Separation of roles to avoid over lapse of duties	4	6.3	87.3
Emphasis on secure internet platform	2	3.2	90.5
Taking legal action on fraudsters	3	4.8	95.2
Emphasis on employee background checks before employment	1	1.6	96.8
Improved internal audit measures and card reconciliations	1	1.6	98.4
Increased physical checks on staff to reduce entry of card reading devices.	1	1.6	100
Total	63	100	100

Literature reviewed also identified information sharing related to card fraud as another current means of addressing this fraud (Cheney et al., 2012). They cited the Information Sharing and Analysis Centre (ISAC) and the Financial Services Information Sharing & Analysis Centre (FS-ISAC) in the U. S, which were formed to specifically facilitate information sharing on physical and cyber security threats and data breaches in the public and private sectors. However, only 4.8% of the respondents indicated that information sharing by hotels will assist in addressing credit card fraud challenges in the hotel industry in Kenya. This finding is attributed to the findings in the Deloitte Financial Crimes Survey report 2013, which stated that victims of credit card fraud fear to report incidences of fraud due to fear of reputational costs and impacts (Deloitte, 2013). Reputational risk is a key risk to the hotels as it has a direct impact on their occupancies and financial performance.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

An overall summary of the research is presented in this chapter. Emphasis is placed on ensuring that each objective which formed the basis of the research has been addressed and ensuring that the research questions are answered adequately. The research limitations encountered in the research are also discussed, highlighting areas that researchers can place emphasis on in future studies.

5.2 Discussions

The research findings show that credit cards are mostly used to settle transactions in the hotels. There is an overall acceptance of credit cards as a mode of payment in the hotels. This is mostly fostered by increased acceptance of credit cards as a mode of payment and increased online and internet-related transactions; facilitated by the provision of a website where clients can make reservations and pay for their bookings online. The provision of a secure card swiping platform also gives an assurance to hotel guests who decide to use the online platforms. The respondents however felt that fear of exposure to fraudulent credit card transactions and insecure card swiping platforms still withhold clients from using their cards to settle transactions.

The respondents agree to the occurrence of credit card fraud in their hotels and most placed the magnitude of fraudulent credit card transactions at between 0 – 10%. The impacts of credit card fraud were identified as financial and reputational. Most respondents (69%) placed the financial impacts of credit card fraud at below Ksh.2 Million, 23% placed this at between Ksh. 2-5 Million while only three respondents placed this loss at over Ksh. 10 Million. A majority (93.5%) of the respondents stated reputation cost as the other impact that hotels face due to credit card fraud. This is felt through increased guest complaints, negative feedback from guests and even bad hotel reviews for instance on TripAdvisor. This finding adds to the already existing literature which relates credit card fraud in hotels to hotel reputation and subsequent decline in financial performance (CHR, Cornell University, 2012).

The respondents felt that to a large extent, the internet and e-commerce activities, lost or stolen credit cards, identity theft and counterfeit credit cards were used to perpetrate credit card fraud and therefore amongst the top factors contributing to credit card fraud in the hotel industry. 17.9% of the respondents stated that card fraud perpetrated via the internet and e-commerce platform were extremely common, 10.3% stated that lost or stolen card used in the fraud was equally extremely common. 23%, 25% and 23% of card fraud transactions were perpetrated through lost or stolen cards, identity theft and internet/e-commerce respectively. Therefore, as cited in the literature reviewed, factors that contribute to card fraud in other industries like banking, financial services and real estate are also prevalent in the hotel industry.

In order to mitigate against credit card fraud in their hotels, respondents stated that they had largely adopted implementation of the PCI DSS requirements, stringent password policies, system interfacing, continuous training for staff, stringent controls for on-line transactions and segregation of duties and clear role separation. 31.7% of the respondents however suggested that in order to address this problem in the hotel industry, the hotels in Kenya should fully implement the PCI DSS requirements so as to create a safe card environment. 23.8% added that staff training and sensitization should also be encouraged while 20.6% of them opined that emphasis should be placed on the security of card information provided by guests for instance through data encryption during transmission and truncation of card numbers. The research findings are in tandem with the observations by Bhatla et al., (2003) and Cheney et al., (2012), who noted that technology-assisted credit card detection and prevention methods are advancing at a rapid rate. They added that fraud mitigation in the credit card industry is to a large extent coordinated by network rules, for instance the PCI DSS guidelines initiated by Euro, Master and Visa Card.

5.3 Conclusion

The findings of this research are of importance to the Hotel industry in Kenya and to the Ministry of Tourism. Credit card fraud indeed does exist in the hotel industry. While the industry has generally embraced and adopted credit cards as a mode of payment, credit

card fraud may be a deterrent in the future given that fraudulent transactions do exist. The impacts of credit card fraud are identified as both financial and reputational. However, reputational impacts are identified as of most concern to the hotels sampled. The factors contributing to card fraud are similar to those identified in literature as contributing to card fraud in other industries e. g retail, banking etc. Bhatla et al., (2003) However, one factor identified by the respondents is that by hotel employees who scheme from card paying clients and pocket cash settlements. This ultimately may tarnish the hotel reputation, besides the financial losses. Various controls are identified to mitigate against card fraud with emphasis placed on the full implementation of the Payment Card Industry Data Security Standards. These standards include amongst others, use of the more secure chip and pin cards, data encryption, and masking of credit card data, secure data storage systems by companies and non-disclosure of credit card details. The Hotel industry in Kenya should embrace the PCI DSS guidelines and continuously train their employees to be alert to fraudsters.

5.4 Limitations

The major limitation of this research lies on the absence of statistics specific to credit card fraud in the hotel industry in non-industrialized countries and more-so locally. High reliance was therefore placed on data available in industrialized countries in reviewing empirical literature. Specific statistics related to credit card fraud in the hotel industry in Kenya was not readily available.

Another limitation is attributed to the fact that since most of the hotels in Kenya are private hotels, mainly owned by individuals, most are unwilling to share information that they feel could have repercussions to them. The question to address the first objective on the impact of credit card fraud was designed such that the respondents provided a range on not specific figures; this was done to avoid non-response. As a result, it was not possible to get statistics over a certain period of time in order to perform a trend analysis.

5.5 Recommendation for Future Research

Future researchers should consider studying the extent of credit card fraud in diverse industries in Kenya including the wider tourism industry in Kenya in order be able to

asses impact of card fraud to the tourism industry viz other industries. This should guide government actors in assessing the industry's most affected by credit card fraud compared to their contribution to the economy, and subsequently in designing and implementing measures to address the challenges. Additionally, future research should consider researching on measures that the industry players can take to encourage information sharing and reporting on the impacts of credit card fraud for instance, through the Ministry of Tourism so that statistics are available for the industry.

REFERENCES

- ACFE (2007). The 2007 Fraud Examiners Manual. Association of Certified Fraud Examiners. Texas: Austin.
- Anastas, J. (1999). *Research Design for Social Work and the Human Services. Chapter 5, Flexible Methods: Descriptive Research*. New York: Columbia University Press.
- Anderson, C. (2012). *Impacts of Social Media on Lodging Performance*. Retrieved 5th November, 2013, from <http://www.hotelschool.cornell.edu/research/chr/pubs/reports/abstract-16421.html>
- Bai, F. & Chen, X. (2013). Analysis on the New Types and Countermeasures of Credit Card Fraud in Mainland China. *Journal of Financial Crime*, 20(3), 267-271.
- Baker, K., D'Amato, J., & Sheridon, P. (2008). Credit Card Fraud: Awareness and Prevention. *Journal of Financial Crime*, 15(4), 398-410. Retrieved 2nd September, 2013 from Emerald database.
- Becker, R., Volinsky, C., & Wilks, A. (2010). Fraud Detection in Telecommunications: A Historical Perspective and Lessons Learned. *Technometrics*, 52, 20–33.
- BFID (2013). Banking Fraud Investigations Department Report, 2013, Author
- Bhatla. T., Prabhu. V. & Dua. A. (2003). Understanding Credit Card Frauds. Retrieved 24th December, 2013 from http://www.popcenter.org/problems/credit_card_fraud/PDFs/Bhatla.pdf.
- Bjelopera. J. & Finklea. K. (2012). Organized Crime: An Evolving Challenge for U.S. Law Enforcement. Retrieved 12th December, 2013, from <https://www.fas.org/sgp/crs/misc/R41547.pdf>.
- Broody, R., Gonzales, K. & Oldham, D. (2013). Wi-Fi Hotspots: Secure or Ripe for Fraud? *Journal of Forensic & Investigative Accounting*, 5(2).
- Carmines, E., & Zeller, R. (1991). *Reliability and Validity Assessment*. London: Sage Publications Ltd.
- Choi, K. (2010). *Risk Factors in Computer-Crime Victimization*. El Paso, TX: LFB Scholarly Publishing LLC.
- Conradt, C. (2011). Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. *International Journal of Cyber Criminology*, 6 (1), 912-923.

- Croson, D., & Jacobides, M. (1997). Agency Relationships and Monitoring in Electronic Commerce. *International Journal of Electronic Commerce*, 1(3), 65-82.
- Delamaire, L., Abdou, H., & Pointo, J. (2009). Credit card fraud and detection techniques: a review. *Banks and Bank Systems*, 4(2).
- Ducey, J. & Gilger L. (2013) Thirty Eight Percent of all Credit Card Fraud Involves the Hotel Industry. Retrieved 1st September, 2013, from <http://hospitalitybusinessnews.com>.
- Dukhi. R. & Dahake. S. (2012). Overview of Fraud Prevention & Management, *International Journal of Computer Applications*.
- EMV (2013). About EMV. Retrieved 25th October, 2013, from https://www.emvco.com/about_emv.aspx
- Financial Crimes Survey Report 2013: Where is the Exposure? Retrieved 7th December, 2013 from <http://www.deloitte.com/assets/Dcom-Kenya/Local%20Assets/Documents/Deloitte%20Financial%20Crimes%20Survey%20Report.pdf>.
- Freeman, R. (2010). *Strategic Management: A Stakeholder Approach*. New York. Cambridge University Press.
- Gilbert, J. & Archer, N. (2012). Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours, *Journal of Financial Crime*, 19(1), 20-26.
- Gill, M., Moon, C., Seaman, P., & Turbin, V. (2002). Security Management and Crime in Hotels, *International Journal of Contemporary Hospitality Management*, 14(2), 58-64.
- Given, L. M. (2008). The SAGE Encyclopedia of Qualitative Research Methods. Retrieved 20th January, 2014 from <http://srmo.sagepub.com/view/sage-encyc-qualitative-research-methods/SAGE.xml>
- Hancock, B. (2002). *An Introduction to Qualitative Research*. Retrieved 20th January, 2014 from http://faculty.cbu.ca/pmacintyre/course_pages/MBA603/MBA603_files/IntroQualitativeResearch.pdf.
- Hayward. K. (2007). Situational Crime Prevention and its Discontents: Rational Choice Theory versus the 'Culture of Now. *Social Policy and Administration*, 41(3), 232-250.

- Hinduja, S., & Schafer, J. (2009). US cyber crime units on the world wide web. Policing, *An International Journal of Police Strategies and Management*, 32(9), 278 – 295.
- Identity Fraud Survey Report (2012). Retrieved 28th September, 2013, from <https://www.javelinstrategy.com>
- Jensen, M. & Meckling, W. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, *Journal of Financial Economics*, 3(4), 305-360.
- Kefee, B. (2013). Thieves Develop New Way to Get Credit Card Numbers at Hotels. Retrieved 25th September, 2013, from, <http://www.10news.com/money/consumer/thieves-develop-new-way-to-get-credit-card-numbers-at-hotels>.
- Kenya Facts and Figures (2012). Retrieved 5th November, 2013, from <http://knbs.or.ke/downloads/pdf/Kenyafacts2012.pdf>.
- KAHC (2014). Kenya Hotel Guide 2014, Author.
- Kimani, M. & Thiongo, P. (2013, November 2). Shock As Kenyan Bank Losses to Fraud Triple to Sh1.6bn. The East African. Retrieved 7th December, 2013, from <http://www.theeastafrican.co.ke/news/Kenyan-banks-lose--18-8m-to-savvy-fraudsters/-/2558/2057524/-/gfy7g3z/-/index.html>
- KIPPRA (2013). Kenya Economic Report 2013, Author.
- Kothari, C. (2004). *Research Methodology Methods & Techniques (2nd ed.)*. New Delhi: New Age International (P) Ltd
- Leblebici, H. (2012). The Evolution of Alternative Business Models and the Legitimization of Universal Credit Card Industry: Exploring the Contested Terrain Where History and Strategy Meet. *Advances in Strategic Management*, 29, 117-151.
- Mason, A., (1998). Computers and Productivity, *Public Productivity Review*, pp. 70-84.
- McQuade, S. (2006). *Understanding and Managing Cyber Crime*. Boston, MA: Pearson Education Inc.
- Ministry of Tourism (2010). *Tourism Performance Overview*. Retrieved 27th September, 2013, from <http://www.tourism.go.ke>
- Newark. N. J. (2013). Eighteen People Charged in International \$200 Million Credit Card Fraud Scam. Retrieved 12th January, 2013, from <http://www.fbi.gov>

- Ngigi, George. (2012). Global Electronic Card Firms Shun Kenya Over Fraud. Retrieved 9th November, 2013, from <http://www.businessdailyafrica.com/Global-electronic-card-firms-shun-Kenya-over-fraud/-/539552/1328186/-/teq0dt/-/index.html>
- Number of ATMs, ATM Cards, & POS Machines. Retrieved 2nd November, 2013, from <http://www.centralbank.go.ke/index.php/nps-modernization/retail-payments-submenu/payment-card-submenu>
- Ogwueleka, F. (2011). Data Mining Application in Credit Card Fraud Detection System, *Journal of Engineering Science and Technology*, 6(3), 311-322.
- Otini, R. (2012, February 17). Africa Investors to Meet In Kigali In March Over Cyber. Business Daily Africa. Retrieved 1st September, 2013, from <http://www.businessdailyafrica.co.ke>.
- PCI Security Standards Council (2013). Retrieved 6th November, 2013, from <https://www.pcisecuritystandards.org/>
- Penemon Institute (2009). *2009 Annual Study: Cost of a Data Breach*. Retrieved 28th September, 2013 from www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CO_DB_09_012209_sec.pdf - “.”
- Percoco, N. (2010). *Global Security Report 2010: Analysis of Investigations and Penetration Tests*. Retrieved September 2nd, 2013, from <https://www.trustwave.com/spiderlabs>
- Percoco, N. (2011). *Global Security Report 2011: Analysis of Investigations and Penetration Tests*. Retrieved September 2nd, 2013, from <https://www.trustwave.com/spiderlabs>
- Poulsen, K. (2009). *Credit Card Skimming Survey: What's Your Magstripe Worth?* *Wired Magazine Threat Level blog*. Retrieved 2nd October, 2013 from www.wired.com/threatlevel/2009/10/florida_skimming.
- Prabowo, H. (2012). A Better Credit Card Fraud Prevention Strategy for Indonesia, *Journal of Money Laundering Control*, 15(3), 267-293.
- Press, D. (2013). *Skimming and Bust-outs*. Retrieved 5th January, 2014, from http://www.greensheet.com/gs_archive.php?issue_number=030702&story=11
- Pulina, M. (2010). Consumer Behaviour in the Credit Card Market: A Banking Case study, *International Journal of Consumer Studies*, 35, 86-94.

- Pulina, M. & Paba, A. (2010). *A discrete choice approach to model credit card fraud*. Munich Personal RePEc Archive. Blackwell Publishing, U.K
- Rini. B. (2002). *Online Credit Card Fraud*. Retrieved 7th December, 2013, from <http://www.windowsix.com>
- Shahonya, E. (2014, February 1). EMV Cards to Shield Banks from Fraud. The East African. Retrieved 7th December, 2013, from <http://www.theeastafrican.co.ke/news/-/2558/2169304/-/763k9ez/-/index.html>
- Sim. S. (2000). Effective Countermeasures against Economic Crime and Computer Crime. *Resource material series* no. 55: 103-116.
- Spano, R. & Frielich, J. (2009). An assessment of the empirical validity and Conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005, *Journal of Criminal Justice*, 37(3), 305-314
- Sullivan. R. (2010). *The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options*. Retrieved 20th December, 2013, from http://weis2010.econinfosec.org/papers/panel/weis2010_sullivan.pdf
- Tedder, K. (2009). *Now You See It, Now You Don't: A Review of Fraud Costs and Trends*. Retrieved 7th December, 2013, from http://www.firstdata.com/downloads/thought-leadership/fd_fraudcostsandtrends_whitepaper.pdf
- Trip Advisor (2013). Retrieved 5th November, 2013, from <http://www.tripadvisor.com/>
- UNWTO (2013). UNWTO World Tourism Barometer, 11. Retrieved 21st April, 2014, from <http://www.e-unwto.org/content/v072pk012j143j52/fulltext.pdf?page=1>
- Verizon 2012 Data Breach Investigations Report. (2012). Retrieved 28th September, 2013, from www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

APPENDICES

Appendix 1: The Kenya Gazette, 13th June, 2003

THE KENYA GAZETTE

Published by Authority of the Republic of Kenya

(Registered as a Newspaper at the G.P.O.)

Vol. CV—No. 62

NAIROBI, 13th June, 2003

Price Sh. 40

GAZETTE NOTICE No. 3976

THE HOTELS AND RESTAURANTS (CLASSIFICATION OF HOTELS AND RESTAURANTS) REGULATIONS, 1983

CLASSIFICATIONS

IN EXERCISE of the powers conferred by regulations 3 and 7 of the Hotels and Restaurants (Classification of Hotels and Restaurants) Regulations, 1983, the Hotels and Restaurants Authority classifies the hotels and restaurants listed in the schedule in the manner specified.

SCHEDULE

Name of hotel	Address	No. of beds	Location
TOWN HOTELS			
<i>Five Star:</i>			
Hotel Intercontinental	P.O. Box 30353-00200, Nairobi	770	Nairobi
Grand Regency Hotel	P.O. Box 57349, Nairobi	388	Nairobi
Hilton Hotel	P.O. Box 30624-00100, Nairobi	353	Nairobi
The Norfolk Hotel	P.O. Box 40064	334	Nairobi
Nairobi Serena	P.O. Box 46302, Nairobi	283	Nairobi
The Stanley	P.O. Box 30680, Nairobi	434	Nairobi
Safari Park Hotel	P.O. Box 45038, Nairobi	285	Nairobi
<i>Three Star:</i>			
The Bounty Hotel	P.O. Box 75200, Nairobi	400	Nairobi
Fair View Hotel	P.O. Box 40842, Nairobi	163	Nairobi
Marble Arch Hotel	P.O. Box 12234, Nairobi	77	Nairobi
Landmark Hotel	P.O. Box 14287, Nairobi	242	Nairobi
Holiday Inn	P.O. Box 66807, Nairobi	342	Nairobi
Windsor Golf Country Club	P.O. Box 45587, Nairobi	260	Nairobi
Nairobi Safari Club	P.O. Box 43564, Nairobi	282	Nairobi
Utalii Hotel	P.O. Box 31052, Nairobi	103	Nairobi
Quangan Hotel	P.O. Box 24, Nyeri	90	Nyeri
Ambassadeur Hotel	P.O. Box 30399, Nairobi	190	Nairobi
Sportsman Arms Hotel	P.O. Box 3, Nanyuki	125	Nanyuki
<i>Two Star:</i>			
Panafic Hotel	P.O. Box 30486, Nairobi	46	Nairobi
Silver Springs Hotel	P.O. Box 61367, Nairobi	188	Nairobi
Midland Hotel	P.O. Box 908, Nakuru	65	Nakuru
Tex Hotel	P.O. Box 71, Kericho	77	Kericho
Hotel Sirikwa	P.O. Box 3361, Eldoret	210	Eldoret
Hotel Kanate	P.O. Box 1369, Nakuru	146	Nakuru
Hotel Boulevard	P.O. Box 42831, Nairobi	140	Nairobi
Eel Hotel	P.O. Box 36, Elburgon	78	Elburgon
Six Eighty	P.O. Box 41436, Nairobi	680	Nairobi
Sports View Hotel	P.O. Box 74194, Nairobi	104	Nairobi

Appendix 2: List of Five and Four Star Hotels in Nairobi

	HOTEL	Star Ranking
1.	Nairobi Serena Hotel	Five Star
2.	The Boma Nairobi	Five Star
3.	Red Court Nairobi	Four Star
4.	Sarova Stanley	Five Star
5.	Villa Rosa Kempinski	Five Star
6.	Sankara Nairobi	Five Star
7.	Tribe Hotel	Five Star
8.	Crowne Plaza Hotel Nairobi	Four Star
9.	Best Western Premier Nairobi	Four Star
10.	Eka Hotel Nairobi	Four Star
11.	Southern Sun Mayfair Nairobi	Four Star
12.	Fair View Hotel	Four Star
13.	Hemingway's Nairobi	Five Star
14.	Fairmont The Norfolk	Five Star
15.	InterContinental Nairobi	Five Star
16.	The Panari Hotel	Five Star
17.	Hilton Nairobi	Five Star
18.	Laico Regency Inn	Five Star
19.	Ole-Sereni Nairobi	Four Star
20.	Safari Park Hotel	Five Star
21.	Holiday Inn	Four Star
22.	Palacina Residence & Suites	Four Star
23.	Windsor Golf Hotel & Country Club	Four Star
24.	Nairobi Safari Club	Four Star
25.	Pride Inn Hotel Lantana Suites	Four Star

Appendix 3: List of Target Hotels

	HOTEL	Star Ranking
1.	Nairobi Serena Hotel	Five Star
2.	The Boma Nairobi	Five Star
3.	Red Court Nairobi	Four Star
4.	Sarova Stanley	Five Star
5.	Villa Rosa Kempinski	Five Star
6.	Sankara Nairobi	Five Star
7.	Tribe Hotel	Five Star
8.	Crowne Plaza Hotel Nairobi	Four Star
9.	Best Western Premier Nairobi	Four Star
10.	Eka Hotel Nairobi	Four Star
11.	Southern Sun Mayfair Nairobi	Four Star
12.	Fair View Hotel	Four Star

	HOTEL	Star Ranking
13.	Hemingway's Nairobi	Five Star
14.	Fairmont The Norfolk	Five Star
15.	InterContinental Nairobi	Five Star
16.	The Panari Hotel	Five Star
17.	Hilton Nairobi	Five Star
18.	Laico Regency Inn	Five Star
19.	Ole-Sereni Nairobi	Four Star
20.	Safari Park Hotel	Five Star

Appendix 4: Questionnaire

QUESTIONNAIRE

SECTION 1: GENERAL INFORMATION

Position/ Job title

Department

Years of experience in the Hotel Industry

☐ 0-5 years ☐ 6-10 years ☐ 11-15 years ☐ 16-20 years ☐ over 21 years

SECTION 2: CREDIT CARD USE AND THE INCIDENCE OF CREDIT CARD FRAUD

1. To what extent are credit cards used to settle transactions in the hotel? Please rank extent using the scale below; where 5 implies a great extent and 1 implies rare use.

1	2	3	4	5
☐	☐	☐	☐	☐

2. The following factors have been identified in literature as some of the factors influencing the level of use of credit cards as a mode of payment. Using the scale below, please rank from the most contributing factor to the least; where 5 implies strongly agree and 1 implies strongly disagree.

Reasons for Increased Use	Rank	Reasons for Decreased Use	Rank
Easy availability of credit		Fear of exposure to fraudulent charges	
Increased acceptance of C/card as a mode of payment		Non-acceptance of credit cards as a mode of payment	
Increased on-line/internet transactions		Uncertainty over security of credit card swiping platforms	
Decreased savings/ability to save		Market preference for debit cards	
Focus on secure credit card platforms		Desire for a simple lifestyle	

3. Have you experienced any incidence (s) of credit card fraud in the hotel?

Yes ☐ No ☐

4. If Yes, what is the magnitude of fraudulent/attempted fraudulent card transactions in the hotel as a percentage of total credit card transactions?

- i) 0 – 5% ☐
- ii) 5 – 10% ☐
- iii) 10 – 20% ☐
- iv) 20 – 30% ☐
- v) 30 – 40% ☐
- vi) 40 – 50% ☐
- vii) Over 50% ☐

5. Academic literature has identified the following as some of the factors contributing to credit card fraud in the hotel industry (*ways through which credit card fraud occurs in the hotel Industry*) Using a scale of 1 – 5, please rank the factors indicated below, where:

- 5 – Extremely common
- 4 – Most common
- 3 – Common
- 2 – Slight cases seen
- 1 – Rare

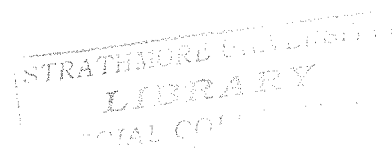
Factors/ Ways Through Which Credit Card Fraud Occurs in the Hotel	Rank
a) There are incidences where fraudsters use/attempt to use lost or stolen credit cards to pay for their bills in the Hotel	
b) There are incidences where fraudsters use/attempt to use other people's credit cards to pay their bills in the hotel by falsifying their identities	
c) There are incidences where fraudsters use/attempt to use counterfeit cards to settle their bills in the hotel	
d) There are incidences where fraudsters provide false financial information in order to be granted credit by the hotel	
e) There are incidences where hotel employees collude/attempt to collude with fraudsters to abet credit card fraud	
f) There are incidences where customers themselves collude/attempt to collude with fraudsters to abet credit card fraud in the hotel	
g) There are incidences where the internet and E-commerce activities have been used as a medium to foster credit card fraud in the hotel	
h) There are incidences where fraudsters have attempted to clone or set up sites similar to that of the hotel for fraudulent purposes	
i) There are incidences where fraudsters have/have attempted to falsify hotel email addresses to defraud potential customers (phishing)	

6. Aside from the factors indicated above, in what other ways is credit card fraud/fraudulent credit card activities perpetrated in your hotel?

.....
.....
.....

7. What is the annual estimated financial loss arising from credit card fraud to the hotel?

- ☐ Less than Kshs.2,000,000 p.a
☐ Between Kshs.2,100,000 - 5,000,000 p.a
☐ Between Kshs.5,100,000 - 10,000,000 p.a
☐ Above Kshs. 10,000,000 p.a



8. Aside from financial losses, what other impacts of credit card fraud occurrences has the hotel witnessed?

.....
.....

9. The following possible measures have been identified as ideal to address credit card fraud in the hotel industry. Using a scale of 1 – 5, please rank the measures that have been most commonly adopted; where 5 is the most common and 1 is the least common:

Measures

Ranking

- | | |
|---|--------------------------|
| 1. Implementation of the Payment Card Industry Data Security Standards | ☐ |
| 2. System interfacing to prevent manual intervention of entries | ☐ |
| 3. Stringent password policy controls to avoid system abuse | ☐ |
| 4. Stringent controls in the on-line booking platform e. g strong firewalls | ☐ |
| 5. Continuous training to staff, Guest Profiling | ☐ |
| 6. Centralised duties and controlled system rights | ☐ |

10. What in your view needs to be done to address the problem of credit card fraud in the hotel industry in Kenya?

.....
.....
.....
.....

Thank you for participating

Appendix 5: Introduction Letter

Strathmore University

8th, March 2014

To whom it may concern

RE: Yego, Peninah Cherono. No: 070854:

Peninah Yego is a postgraduate student in our Master of Commerce (MCom) Programme. In partial fulfilment of the MCom degree, students are required to carry out a research project and write a thesis on a contemporary subject within their field of specialization. Among other activities, the project involves data collection and analysis.

Ms. Yego is requesting to gather information to be used in her research. The information she will obtain from your organization will be used for academic purpose only and will be kept confidential. The results of the survey will be in summary form and will not disclose any individual, organization name or organization information in any way.

The research study is entitled: “Extent of Credit Card Fraud in the Hotel Industry in Kenya”.

We hope that your organization can assist by providing information to the above named student.

Yours faithfully,

Carolyne Nafula,

MCom Coordinator,

School of Management and Commerce