BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

CHALLENGES IN CURBING CARD FRAUDS IN BANKS. A CASE OF ABC BANK FROM JANUARY 2017 TO DECEMBER 2018

BY

Ndabezinhle Moyo

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELORS OF BUSINESS ADMINISTRATION (S) DEGREE IN POLICE AND SECURITY STUDIES OF BINDURA UNIVERSITY OF SCIENCE EDUCATION

DEPARTMENT OF POLICE STUDIES AND FINANCIAL INTELLIGENCE
“Challenges in curbing card fraud in banks. A case of FBC Bank from January 2017 to December 2018.”

I certify that this dissertation meets the preparation on guidelines as presented in the college guide and instruction of typing dissertation.

.................................................    ..................................
Student’s Signature       Date

This dissertation is suitable for submission to Bindura University of Science Education. This dissertation should be checked for conformity with the Bindura University of Science Education guidelines.

....................................................    ..........................................
Supervisor’s Signature      Date

I certify to the best of my knowledge that the required procedures have been followed and the preparation have been met for the dissertation.
 RELEASE FORM

Name of author: Ndabezinhle Moyo

Title of Project: “Challenges in curbing card fraud in banks. A case of FBC bank from January 2017 to December 2018.”

Program: Bachelor of Business Administration Honours
Degree in Police and Security Studies of Bindura University of Science Education.

Year Granted: December 2019

Permission is hereby granted to Bindura University of Science Education to produce copies of this project and to sell copies for private, scholarly or scientific research purpose only. The author does not reserve the other publication rights of the project nor may extensive extracts from it be printed or otherwise reproduced without the author’s written permission.

Signed

Permanent Address: 19983 Zengeza 4
Chitungwiza
DECLARATION

I, Ndabezinhle Moyo declare that this research project is my own work and has not been copied or lifted from any source without the acknowledgement of the source.

………………………………………  ………………………………………
Signed                          Date
DEDICATION

I dedicate this dissertation to my loving family. This is to the love we share, and the friendship that no one can ever replace.
ABSTRACT

This research study was an investigation on the challenges in curbing card fraud in the banks using a case study of FBC Bank for the period from January 2017 to December 2018. It was guided by the following objective questions; to establish the causes of card fraud in the banks; to ascertain factors impeding effective policing of card fraud in the Zimbabwe Republic Police, to establish ways of mitigating challenges in policing card fraud in both the banks and the police, and to recommend on strategies to curb card fraud. The research was conducted after an observation that the card fraud was on the increase to a level of becoming an epidemic. The researcher used the mixed research approach, that is to say, both qualitative and quantitative research approaches were used. The descriptive survey research design was used and questionnaires and interviews were used to collect data. A sample of 70 respondents was used comprising 12 CCD officers, 40 card fraud complainants for the year 2018 and 18 FBC bank employees using stratified simple random sampling technique. The major findings of the study revealed that greed is the most common reason of commission of the crimes of card fraud while low detection and poverty also influenced commission of card fraud. The most commonly used strategies to address card fraud are specialized card fraud management training, inter-agency policing and community policing initiatives, these strategies are used by both CCD and FBC Bank in fighting the card fraud crime. From the findings, it was concluded that CCD is faced with operational challenges which were identified as complexity of crime, skills gap, and technology as well as resource constraints. In addition, there are challenges in legislation which trivialises card fraud identified by classifying it in the category of a mere statutory violation under computer related crimes as opposed to a purely advanced form of fraud. From the conclusions, the researcher recommended that the criminal justice system must collaborate with the legislature to review and revise the current sentencing of card fraudsters
to ensure that deterrent sentences are passed onto card fraud perpetrators; continued upgrading of skills and collaboration of all stakeholders.
I am grateful to my supervisor Mr. F.B Gombarume who has tirelessly and meticulously edited over and over this research study with such professional competence and patience. Over and above all, I thank God Almighty for according me with the zeal, determination and an array of possibilities, enabling me to complete this research study successfully.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Numbering</th>
<th>Details</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Approval Form</td>
<td>i</td>
</tr>
<tr>
<td></td>
<td>Release Form</td>
<td>ii</td>
</tr>
<tr>
<td></td>
<td>Declaration Form</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>Dedication Form</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>Abstract</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>Acknowledgements</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>Table of Contents</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>List of Tables</td>
<td></td>
</tr>
<tr>
<td></td>
<td>List of Figures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>List of Appendices</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CHAPTER ONE: INTRODUCTION</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Background of the study</td>
<td>1</td>
</tr>
<tr>
<td>1.3</td>
<td>Statement of the problem</td>
<td>4</td>
</tr>
<tr>
<td>1.4</td>
<td>Purpose of the study</td>
<td>4</td>
</tr>
<tr>
<td>1.5</td>
<td>Research objectives</td>
<td>4</td>
</tr>
<tr>
<td>1.6</td>
<td>Research questions</td>
<td>6</td>
</tr>
<tr>
<td>1.7</td>
<td>Research hypothesis</td>
<td>6</td>
</tr>
<tr>
<td>1.8</td>
<td>Assumptions</td>
<td>6</td>
</tr>
<tr>
<td>1.9</td>
<td>Delimitations</td>
<td>6</td>
</tr>
<tr>
<td>1.10</td>
<td>Significance of the study</td>
<td>6</td>
</tr>
<tr>
<td>1.11</td>
<td>Definition of Terms</td>
<td>8</td>
</tr>
<tr>
<td>1.12</td>
<td>Organization of the study</td>
<td>8</td>
</tr>
<tr>
<td>1.13</td>
<td>Summary</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td><strong>CHAPTER TWO: LITERATURE REVIEW</strong></td>
<td>10</td>
</tr>
<tr>
<td>2.1</td>
<td>Introduction</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>Purpose of literature review</td>
<td>10</td>
</tr>
<tr>
<td>2.3</td>
<td>Card Fraud conceptual framework</td>
<td>10</td>
</tr>
<tr>
<td>2.4</td>
<td>Theoretical framework</td>
<td>13</td>
</tr>
<tr>
<td>2.5</td>
<td>Types of credit card fraud</td>
<td>16</td>
</tr>
<tr>
<td>2.6</td>
<td>Challenges in curbing card fraud</td>
<td>19</td>
</tr>
<tr>
<td>2.7</td>
<td>Measures to improve policing card fraud</td>
<td>22</td>
</tr>
<tr>
<td>2.8</td>
<td>Summary</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td><strong>CHAPTER THREE: RESEARCH METHODOLOGY</strong></td>
<td>27</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>27</td>
</tr>
<tr>
<td>3.2</td>
<td>Research design</td>
<td>27</td>
</tr>
<tr>
<td>3.3</td>
<td>Population and sampling</td>
<td>28</td>
</tr>
<tr>
<td>3.4</td>
<td>Sample</td>
<td>28</td>
</tr>
<tr>
<td>3.5</td>
<td>Research instruments</td>
<td>28</td>
</tr>
</tbody>
</table>
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table number</th>
<th>Table Title</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1.1</td>
<td>Card fraud cases reported at CCD 2016 TO 2018</td>
<td>4</td>
</tr>
<tr>
<td>Table 4.2</td>
<td>Demographic data</td>
<td>36</td>
</tr>
<tr>
<td>Table 4.3</td>
<td>Respondents distribution by age</td>
<td>36</td>
</tr>
<tr>
<td>Table 4.4</td>
<td>Respondents distribution by education</td>
<td>37</td>
</tr>
<tr>
<td>Table 4.5</td>
<td>Card fraud prevalence</td>
<td>39</td>
</tr>
<tr>
<td>Table 4.6</td>
<td>Respondents reason for increase in card fraud</td>
<td>39</td>
</tr>
<tr>
<td>Table 4.7</td>
<td>Current strategies to curb card fraud</td>
<td>41</td>
</tr>
<tr>
<td>Table 4.8</td>
<td>Respondents view on operational challenges</td>
<td>42</td>
</tr>
<tr>
<td>Table 4.9</td>
<td>Respondents view on legislation of card fraud</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>management</td>
<td></td>
</tr>
<tr>
<td>Table 4.10</td>
<td>Respondents view on ways to improve card fraud</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>management</td>
<td></td>
</tr>
</tbody>
</table>
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure Number</th>
<th>Title of Figure</th>
<th>Page number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 4.1</td>
<td>Questionnaire distribution response rate</td>
<td>35</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Respondents response on card fraud</td>
<td>40</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Respondents view on effectiveness of current strategies</td>
<td>41</td>
</tr>
</tbody>
</table>
# LIST OF APPENDICES

<table>
<thead>
<tr>
<th>Numbering</th>
<th>Title of Appendix</th>
<th>Page number</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Introductory Letter to all respondents</td>
<td>60</td>
</tr>
<tr>
<td>B</td>
<td>Questionnaire for police officers and Bank employees</td>
<td>61</td>
</tr>
<tr>
<td>C</td>
<td>Interview guide for complainants</td>
<td>63</td>
</tr>
<tr>
<td>D</td>
<td>Sample of a cloned FBC Bank card on a BancABC card</td>
<td>64</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction
This chapter covers background of the study, statement of the problem, research objectives, hypothesis, research questions and importance of the study, delimitation and limitation of the study on the increase in card fraud cases.

1.2 Background of the Study
The idea of paying for goods and services electronically is not a new one. Since 1970s and early 1980s, a variety of schemes have been proposed to allow payment to be effected across a computer network (Dara and Gundemoni, 2006). After a period of exponential growth, 930 million people have Internet access worldwide. The electronic payment system started at the end of 1966 and in the earlier part of 1977, a variety of different payment methods was developed by both the academic researchers and commercial interests. Some of these were launched on the market and failed to reach a critical mass. Cyber cash and digital cash were also launched payment systems that achieved quite extensive deployment but failed to generate an economic return. At the same time many companies started up new methods of payments (O’Mahony, 1997).

The emergence of electronic commerce has brought in its wake some major security concerns (Dara and Gundemoni, 2006). Electronic payment has dominated and attracted much attention in recent times as all major stakeholders, thus payment operators, electronic card manufacturers as well as cardholders continue to seek for effective means of combating the threats of internet frauds and more specifically credit cards frauds. Of the security issues facing banks everywhere, prevention of credit cards frauds has always been a high priority (Dara and Gundemoni, 2006).

Card fraud has taken Zimbabwe by storm. Card fraud has become a crime of concern due to the large amounts of financial losses incurred by individuals and
the nation at large. Card fraud takes many forms like fraudently posing as a bank, an insurance company, an online store, forgery, altering cheques, accounting card fraud, wire transfer card fraud, fraudulently using stolen ATM cards among others (Unogbro and Idolor, 2007). The card fraud cases range from bogus property sellers, bogus insurance companies, stock-broking scams, internet card fraud, partnership card fraud, and bogus online shops. Card fraudsters manipulate any institution from posing as an online store to even posing as a bank (Unogbro and Idolor, 2007). Unsuspecting victims are then swindled of their money when they transact with these fraudulent organised syndicates. In Zimbabwe card fraud cases are on the increase as a result of the current cash shortages and use of plastic money as a means of transaction.

In an interview with Barnabas Vera, the Divisional Director Group Audit and Security at FBC Bank, he mentioned that during the period January 2018 to December 2018 alone, a total of 83 cases were recorded from both FBC Bank and Building Society, causing a prejudice of $298,663.00. It is worth noting that, during the month of October 2018 alone; a total of 11 One Time Password (OTP) fraud cases were received, which is a significant rise on the number of such cases received in a single month. In the OTP fraud category, the fraudster only requires the mobile number of the targeted client, and logs that mobile number on the bank mobile platform using own device. As a result, a genuine OTP message is generated and sent to the targeted client’s mobile device. The fraudster immediately makes a follow up by phoning the targeted client, misrepresenting to be a bank employee and in the process requesting back the OTP number which would have been sent to the victim’s number. The victim would be convinced by the trickster that some system upgrade and security enhancements are being carried out by the bank. The victim would unsuspectingly supply the current PIN in use, thereby enabling the fraudster full control and access to transact on the account.

In the majority of card fraud cases, complainants claimed to have been in possession of their ATM cards at the time the disputed transactions would have occurred. Such developments are in sync with (Haller and Melrose, 2019), who is of the view that when the economy continues to heavily depend on electronic
transactions, unscrupulous individuals take it as an opportunity to swindle unsuspecting customers and organizations of their hard earned cash card fraudulently.

Card fraud poses threats to the success of economic development in that direct international investment may be lost in a country as investors fear for their money (Haller and Melrose, 2014). This position was demonstrated by a complaint by Chesani Jaïdi, an FBC Bank account holder who disputed POS transactions done between 15 December 2018 and 27 December 2018, amounting US$98,764.20, at the time he claimed to having been in possession of his ATM card linked to his company bank account. Thus, card fraud makes investors lose trust in the systems of a nation and this is why it is important to address the pandemic. As the economy continues to heavily depend on electronic transactions some people have seen this as an opportunity to swindle unsuspecting customers and organizations of their hard earned cash through credit card manipulation. Victims suffer psychological torment as they stress about their losses (Haller and Melrose, 2014).

Zimbabwe Republic Police (ZRP) in response to this new crime epidemic established a new unit mandated to specifically deal with crimes of card fraud entitled the Commercial Crime Department (CCD). To buttress its support to this section, the ZRP developed a crime strategy which highlights how fraud should be managed by police officers. Accordingly, a public relations section was also established under CCD to complement the efforts of the criminal section in combating card fraud through educational and awareness campaigns. Card fraud like any other crime can only be detected when the communities affected are involved, as such ZRP employs community policing strategies to engage commercial banks, bank customers and other stakeholders in the fight against card fraud. However, these efforts seem to be insufficient to deter crimes of card fraud as they continue to rise thereby, necessitating this study. Below is a graphical illustration depicting the number of cases of card fraud received CCD between the year 2017 and 2018.

Figure 1.1 Card frauds cases reported at CCD in 2016, 2017 and 2018.
Figure 1.1 above shows that in the year 2016 were 390 card fraud cases were reported, in 2017 a total of 420 cases of card fraud were reported while in 2018 the cases of card fraud received increased cumulatively by 190 (33%) to 580 cases. FBC Bank accounted for 83 cases reported in 2018, translating to 14% of the reported cases from 19 banks. Thus, the study sought to determine the challenges in curbing card fraud within the banking sector.

1.3 Statement of the Problem

Despite the establishment of the Commercial Crime Department and the Fraud Strategy to curb crimes of card fraud, card fraud within the banking sector continues to increase thereby prompting the researcher to carry out this study. The constant rise on the number of card fraud cases, as illustrated in figure 1.1 is indicative of the problem at hand, hence this research. Police has embarked on intensive card fraud alert awareness campaigns through various media such as Sunday mail, The Outpost, mobile phones in a bid to educate and conscientise the society about card fraud and to be wary of card fraudsters. However, card fraud cases continue to be on the increase and continue to take new forms and different faces.

1.4 Objectives of the Study
The objectives of the study were:

- To establish the causes of card fraud in banks.
- To ascertain factors impeding effective policing of card fraud in the Zimbabwe Republic Police.
- To establish ways of mitigating challenges in policing card fraud in the banks.
- To recommend on strategies to curb card fraud.

1.5 Research questions

This study seeks to answer the following research questions:

- What are the causes of card fraud?
- What are the factors impeding effective policing of card fraud?
- What measures can be put in place to improve policing card fraud?
- What strategies can be used to curb card fraud?

1.5 Research Hypothesis

Card fraud is on the increase in Zimbabwe due to poor detection and corruption in the law enforcement, justice delivery system and the banking sectors.

Assumptions

The underlying assumptions for this study were that,

- The research would be completed in time.
- The respondents participated in the study voluntarily.
- The respondents answered questions asked truthfully.
- These findings can be generalised on the whole banking sector.

1.6 Delimitations

The study was restricted to card fraud cases in the banking sector. The researcher chose FBC Bank as the case study because it had the highest number of reported card fraud cases. Police officers were selected from CCD as they are the ones on the ground policing card fraud and are better able to identify challenges in card fraud policing based on what they face in their day to day operations.

1.7 Limitations
A number of constraints were encountered during the course of the study. These include the following;

**Resource constraints**
These can be explained in terms of costs for transport, stationery and feeding. The researcher travelled to and from the Harare to undertake interviews, administer questionnaires and to gather data from police records. This required cash for transport. To overcome this, the researcher budgeted for these costs prior to the commencement of the study. This plan also covered the demands for food and stationery. He also relied upon a personal laptop for typing and would finance the printing services from his pocket.

**Organisational concerns**
Since card fraud involved some sensitive issues such as corruption and also fears of being investigated, the organisations were not easily giving access to records. The research sought approval from both CCD and FBC Bank. The researcher overcame this problem by giving a clear account of purpose that this research was purely academic was supported by a referral letter from Bindura University of Science Education. The researcher also highlighted the possible benefits the organisations would harness from this research.

1.8 **Significance of the Study**
The study was of importance to various parties in varying ways as highlighted below;

**To the researcher**
This study enriched the researcher in terms of knowledge about the subject. The researcher acquired knowledge from this study that gave him competitive advantage in terms dealing with cases of card fraud and he was less likely to fall a direct victim of card fraud as was before.

**To the banking sector**
The banking sector is set to benefit from the emerging strategies that would in-turn help to safeguard their clients from card fraud thereby increasing client
confidence in the banking sector. The researcher has potential and ability to influence decision making within the banking sector since he is a member of the Inter-Bank Security Managers Liaison Committee, as well as Bankers Association of Zimbabwe. Input and contribution to such platforms shall be from an informed position.

**To the academic world**
This study definitely added value to empirical literature in the subject of card fraud. It also contributed by closing part of the void that had been left by predecessors in the field of study. It also added to library literature and could be used as referral material by students studying card fraud.

**To the Zimbabwe Republic Police (ZRP)**
The law enforcement agents could benefit if they employ the strategies and solutions suggested by this study. Since the researcher is a retired senior officer, ZRP is bound to benefit if it uses the researcher to impart knowledge gathered during the study to serving members who did not have the opportunity to undergo a similar academic study by strategically inviting him as a guest presenter. This may go a long way in improving the organisation’s overall performance and it may end up being ranked better than others in the region and even globally.

**To the Courts of Law**
This may help prosecutors, magistrates and judges to make more informed decisions or judgements especially when passing sentences for card fraud crimes as well as during trials as this study contains what the police representatives feel is falling short with regards to the delivery of the judiciary system in as much as card fraud is concerned. This project may actually lay a hand in improving the efficiency of the judiciary system when handling card fraud cases.

**To an ordinary citizen (individual) and organisations**
The ordinary citizen and organisation will definitely be warned against the effects of card fraud. There is a guaranteed expansion of knowledge on the subject thereby reducing their chances of falling victims of card fraud. They can
also employ the suggested strategies or solutions to protect their financial and related property and also to safeguard against the occurrence of card fraud in their organisations.

**To the government or the state**
This research may influence lawmakers when crafting card fraud related laws as well as when assigning a penal equivalence for each law so flouted. It may also shed light on the extent to which card fraud costs an economy and how and to what extend card fraud derails the economy.

**1.9 Definition of Terms**

**Card fraud:** In terms of Section 167 of the Criminal Law Codification and Reform Act, 9:27 as without authority, manufactures, copies or use of a credit card or debit card, including without reasonable excuses possess any credit card or debit card belonging to another. However, the researcher believes that card fraud is an unlawful act of misrepresentation through use of an illegally obtained credit or debit card with intent to prejudice the legitimate card holder of his or her funds.

**Card fraud Management Strategy:** A plan set out to curb card fraudulent criminal activities.

**1.10 Project Outline**
This research study is divided into five chapters, Chapter one focuses on the problem and its setting. The second chapter reviews related literature on the topic at hand so as to have an in-depth understanding of what other researchers who once researched on the subject are saying concerning the topic. Chapter three focuses on research methodology under subheadings, research design, research approaches, research methods, population and sampling, research instruments, research ethics and research limitations. The fourth chapter deals with data presentation and discussion. In this chapter, data will be presented in tables, analysed and discussed through narration. Data will be analysed in line with objectives to which it was collected. Chapter five looks at conclusion and recommendations drawn from the study findings.
1.11 Chapter Summary

This chapter covered the background of the study, the statement of the problem, research questions and research objectives, assumptions of the study, delimitation and limitations of the study and definition of terms in relation to the increase in card fraud cases. The next chapter will cover literature review to enable the researcher to get views on what others say about the causes of card fraud.
CHAPTER II

LITERATURE REVIEW

2.1 Introduction
The previous chapter covered the problem and its setting. This chapter covers literature review related to the increase in card fraud cases. This chapter covers the purpose of literature review, theoretical review, causes of card fraud, challenges faced in curbing card fraud, strategies and empirical literature review.

2.2 Purpose of literature review
Literature review, according to Cooper and Schindler (2003) is the examination of recent or historical significant research studies in the subject under study. In this study, literature review allowed the researcher to approach the research problems knowledgeably through reading around the proposed area to provide a theoretical framework to the study, to stimulate debate. It also enabled the researcher to establish the research gap as well as gain more insight into the subject under study. This enabled the researcher to generate and refine research ideas.

2.3 Card fraud conceptual framework
The electronic payment (e-payment) is a method of value exchange in electronic commerce, where the value is transferred via the internet and communication technologies. The electronic payment systems have evolved from traditional payment systems and consequently the two types of systems have much in common. Electronic payment systems are much powerful, especially because of the advanced techniques in security that have no analogy in traditional payment systems. An electronic payment system denotes any kind of network service that includes the exchange of money for goods and services. E-payment is conducted in different e-commerce categories such as Business-to-Business, Business-to-Consumer, Consumer-to-Business and Consumer-to-Consumer (O’Mahony, 2001).

Of the security issues facing banks everywhere, prevention of card fraud has always been a high priority, and is set to grow even further in importance. The
level of card fraud has risen significantly over recent years, caused in the main, by the explosion in the number and usage of payment cards and the associated high level of organized card crime activity. For example, over the past decade, fraud losses on UK-issued plastic cards have risen from 100 million pounds to a staggering five billion pounds a year (Tae-Hwan, 2018).

Credit cards are the most popular payment instrument on the internet. The first credit card was introduced in 1939. In 1996 Visa and Master card announced that they were working together to define a protocol that would enable secure bankcard transactions on the internet. This process involves the use of highly secure encryption digital signature techniques, as well as digital certificates. So that there is no export problem because these mechanisms are embedded in the payment process and are not accessible to the users to secure other non-financial information (Tae-Hwan, 2018).

Among the pitfalls of online credit card usage is the prevalence of online credit card fraud. This online credit card fraud can happen in several ways. Numerous types of card fraud have been developed over the years and are regularly committed throughout the world. The most prevalent and commonly known types are counterfeit card fraud. However as new banking channels have opened up, for example internet, phone banking and e-commerce, and the boom in credit card use, crime has migrated to seek any opportunity to attack these new and immature transaction methods (Ezine, 2014).

Card fraud can be defined as deliberate deceit or an act of deception aimed at causing a person or organization to give up property or some lawful right. The Association of Certified Card fraud Examiners (1999) further defines card fraud as the use of one’s occupation for personal enrichment through the deliberate misuse, misapplication or employment of organizational resources or assets. Card fraud can be defined as the card fraudulent conversion and acquisition of money or property by false pretence (FBI, 2004).

In legal terms, card fraud is seen as the act of depriving a person dishonestly of something, which such an individual would or might be entitled to, but for the
perpetration of card fraud (Omachuni, 2009). In its lexical meaning, card fraud is an act of deception which is deliberately practiced in order to gain unlawful advantage. Therefore, for any action to constitute a card fraud there must be dishonest intention to benefit (on the part of the perpetrator) at the detriment of another person or organization (Diamond, 2004). Card fraud usually requires theft and manipulation of records, often accompanied by concealment of the theft. It also involves the conversion of the stolen assets or resources into personal assets or resources. There is a general consensus amongst criminologists that card fraud is caused by three elements called “WOE” (Will, Opportunity and Escape route), (Onibudo, 2007).

For any card fraud to occur there must be a will, an opportunity and exit (escape route). A card fraud will only occur if the perpetrators have the will to commit the card fraud, if the opportunity to commit the card fraud is available and if there is an exit or escape route from relevant sections or institutions that are against card fraud or related deviant behaviour (Onibudo, 2007). Card fraud is a global phenomenon. It is not unique to the banking industry or for that matter, peculiar to only Zimbabwe.

With the crash of major multinational corporations like Enron (in the United States of America) coupled with high level allegations and actual cases of corporate card fraud (Unogbro and Idolor, 2007) many organizations in their attempt to improve their image have resorted to developing ethical guidelines and codes of ethics. The whole essence of these is to ensure that all organizational members irrespective of rank or status, complies with the minimum standard of ethical responsibility in order to promote the reputation of such firms in their chosen industry, earn the goodwill of customers and thus improve their competitive advantage (Unugbro and Idolor, 2007).

In the present Zimbabwean epoch, many youths and elder citizens alike want to make it within the shortest possible time, because banks deal with money, and money related businesses, it is no wonder that they have become the targets of persistent card fraudsters. As naturally expected, card fraud is perpetrated in many forms and guises, and usually has insiders (staff) and outsiders conniving together
to successfully implement the act. The following types which are not in any way completely exhaustive are the most common types of card frauds in Zimbabwe: Computer card fraud, Occupational card fraud, Insurance card fraud and Housing Scams.

According to Onibudo (2007), card fraud losses impact every business, social and moral values as well as the economy at large. Caveat emptor, let the buyer beware, tells half the story; Caveat Venditor, let the seller beware, tells the rest. Card fraud costs are passed on to society through increased customer inconvenience, opportunity costs, unnecessarily high prices, and criminal activities funded by the card fraudulent gains. In short, card fraud is rampant, thus this study sought to investigate causes of card fraud in Zimbabwe.

2.4 Theoretical framework

Causes of card fraud

Perceived profitable opportunity

According to Angier (2002), Donald Cressey (1973) developed a model to explain why people commit card fraud where he posited that individuals commit card fraud when three factors are present: (1) a financial need that cannot be shared, (2) a perceived opportunity for illicit gains, and (3) a personal rationalization of the act. Cressey reportedly asked offenders why they had not committed violations at other times and received three basic replies: “There was no need for it like there was this time”; “The idea never entered my head”; and “I thought it was dishonest then, but this time it did not seem dishonest at first.” Cressey’s ideas have become known as the Card fraud Triangle (Angier, 2002).

The Card fraud Triangle originates from Cressey (1973)’s hypothesis: trusted persons become trust violators when they have any of the six types of “non-shareable” problem that provoke card fraud. These are: inability to pay debts, problems resulting from personal failure, business reversals, physical isolation, status gaining, and employer-employee relations. Individuals rationalized their crimes as non-criminal, justified, or as part of an environment over which the offender had no control. The opportunities for card fraud are always myriad, though
the lack of internal controls over funds is a chief factor. Removing temptation remains the best deterrent of all (Coleman, 2009). This study therefore sought to prove or disprove explanations in Cressey’s Card fraud Triangle theory pertaining to causes of card fraud in Zimbabwe.

- **Association with criminals (criminal minds)**
  Sutherland (1949) asserted that people interacting in close association learn criminal behaviour (Haller and Melrose, 2014). Rather than imagine an individual suffering from a pathological mental condition, Sutherland argued that people learned how to be criminals from pickpockets to corporate embezzlers by consorting with other criminals (Haller and Melrose, 2014). In critique of Freudian psychological distortions, Sutherland (1949), developed the differential association theory which posits that criminal behaviour is learned.

The criminal learning process includes physical techniques and strategies for committing crime as well as the sharing of motives, drives, rationalizations, and attitudes toward crime (Johnston, 2008). In other words, one not only learns how to commit the crime, but why to commit the crime. Chief among the rationalizations, Sutherland (1949) found, was an acquired sense of legal codes as unfair and/or unfavourable. The causes of corporate crime were unrelated to the psychology of its perpetrators, Sutherland (1949) believed, as evidenced by the fact that criminal corporations may continue committing offenses over time while personnel come and go (Johnston, 2008). However, Sutherland (1949) did not consider that management tends to promote people like themselves, so the psychological profile of the typical manager may remain constant through several administrations (Haller and Melrose, 2014). Thus, the researcher in this study sought to investigate whether association with criminals is one of the causes of card fraud in Zimbabwe.

- **Poor working conditions**
  Richard Hollinger and John Clark (1983) surveyed 10,000 American workers for the book, *Theft by Employees*, and concluded that employees steal primarily as a result of workplace conditions (Quinsey, 2006). External factors such as Cressey’s “non-shareable problems” sometimes play a role, but Hollinger and Clark emphasized the structure and behavioural norms of the workplace, declaring that
worker dissatisfaction was the single most determinative factor in provoking acts of card fraud. A person might need funds to pay off a debt, or the person might feel underpaid and motivated to commit card fraud even without an immediate financial need (Quinsey, 2006).

Hollinger and Clark (1983) concluded that the same kinds of employees who engage in other workplace deviance are also principally the ones who engage in employee theft. They found persuasive evidence that slow or sloppy workmanship, sick-leave abuses, long coffee breaks, alcohol and drug use at work, coming in late and/or leaving early were more likely to be present in the employee-thief (Robinson and Bennett, 2012).

➢ **Unequal social structures**

According to Angier (2002), Robert Merton determined that social structures provide the chief motivation for misconduct. Capitalist competition, the importance of money in society, and the erosion of norms that encourage legitimate moneymaking behaviour all encourage individuals to commit crimes (Robinson and Bennett, 2012).

According to Merton, modern industrial societies emphasized the ends (making money) over the means (ethical earning behaviour), producing a state of “anomie,” or normlessness, in its citizens. Without ethical guidance, a person will use any means necessary to attain money and power (Robinson and Bennett, 2012).

Edwin Schur, as quoted by (Gestel and Weisburd, 2000) located the impulse for economic crime in social structures. Thus, Schur asserted that America hosted so much crime because “American society has what might be termed capitalism with a vengeance, a reverence for the values of individualism, competition, and profit of such intensity as to provide incentives to crime that go well beyond a level that must be considered inevitable in a modern complex society.” (Gestel and Weisburd, 2000).
2.5 Types of Credit Card Frauds

Nowadays credit card fraud is the major and one of the biggest threats to business establishments. However to overcome the fraud effectively, it is important to understand the mechanisms of executing a fraud. The credit card fraud makes a group and employs a large number to commit fraud. In simple terms, credit card fraud is defined as 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 (Bhatla, 2013). Credit card frauds are committed through an act of criminal deception by use of unauthorized credit card account or by getting their personal information; illegal or unauthorized use of account for personal gain and misrepresentation of account information to obtain goods or services.

Hacking

In 1980 the term hacking became a buzzword, which was taken to be derogatory and by the misuse or overuse was attached to any form of socially non-acceptable computing activity outside of police society (Lee, 2011). Credit card hacking is harder to do using traditional methods such as decrypting the magnetic stripes and recreating them. Hackers were assumed to be the fringe society of the computing fraternity, who did not know any better and who had obtained access to a technology with which they terrorized the world of communications and computing. The concept of hacking as a methodology to achieve some particular goal has the allusion of working at something by experimentation or empirical means, learning about the process under a review or development by adhoc mechanisms. In hacking a computer, the enhancement of the system is an end in itself (Lee, 2011).

There are different ways of hacking. In an online credit card purchase, the payment data transfers between the customers’ computers or phones and the vendor’s shop over the internet. That raises concerns about credit card online security and identity theft. It is very difficult to get the credit card details, but thousands of credit cards are compromised in a successful attack. The intellectual hackers and poor web-shop security lead to major breaking that are happening frequently (Lee, 2011).
The hackers are the unauthorized user who tries to access over the internet or anyone with direct physical access can commit identity theft by stealing credit card information electronically. Most internet explorer users enjoy the convenient auto complete feature. It remembers data, including credit card information, used to fill in Web forms and saves it in a safe place. The next time when one is required to fill in similar forms, it completes it automatically. The problem is that it is possible to capture and read the contents of protected storage. A fix for this credit card online security weakness was introduced that excluded of credit card and other sensitive fields from auto completion (Lee, 2011).

**Lost/Stolen Cards**
This is when one person loses his or her card or a card is stolen by someone or when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. This is the easiest way for the fraudsters where he or she gets the information of the cardholders without investing in any of the modern technologies. It is perhaps the hardest form of traditional credit card fraud to tackle (Bhatla, 2013).

**Account Takeover**
This type of fraud occurs when the valid customer’s personal information is taken by the fraudsters. The fraudster takes control of a legitimate account by either providing the customer’s account number or the card number. The fraudster then contacts the card issuer, as the genuine card holder, to ask the mail to redirect to a new address. The fraudster reports card lost and asks for a replacement to be sent (Bhatla, 2013). In the Zimbabwean context, this type of fraud has resurfaced in the form of OTP fraud.

**Cardholder-Not-Present**
Cardholder-not-present transactions are performed only on the internet that is remotely, in such kind of frauds, neither the card nor the cardholder is present at the point-of-sale. This take many types of transactions such as orders made over the phone or internet, by mail order or fax. In such transactions, retailers are unable to physically check the card or the identity of the cardholder, which
makes the use unknown and bale to disguise their true identity. The details of the
card are usually copied without the cardholder’s knowledge, collected from the
receipts thrown by the customer or obtained by skimming process. Fraudulently
obtained card details are generally used with fabricated personal details to make
fraudulent cardholder-not-present purchases. This means that while the three or
four digit card security code on the back of the cards can help prevent fraud
where card details have been obtained, but when the card is stolen it will not be
helpful (Bhatla, 2013).

**Fake and Counterfeit cards**
This is another type of fraud where there is creation of counterfeit cards,
together with lost or stolen cards poses highest threat in credit card frauds.
Fraudsters are constantly finding new and more innovative ways to create
counterfeit cards. Fake or counterfeit cards can be created by erasing the
magnetic strip by using the electro-magnet. The fraudster then tampers with the
details on the card so that they match the details of a valid card, which they may
have attained, for example, when the fraudster begins to use the card, the cashier
will swipe the card through the terminal several times, before realising that the
metallic strip does not work. The cashier will then proceed to insert the card
details manually into the terminal. This kind of fraud is having high risk because
the cashier will be looking at the card closely to read the numbers (Bhatla,
2003).

Another way is creating a fake card. Nowadays, there are sophisticated machines
where one can create a fake card from manipulation of the magnetic stripe. This
is the common fraud though fake cards require a lot of effort and skill to
produce. Modern cards are having many security features, all designed to make
it difficult for fraudsters to make good quality fraudulent. After introducing the
holograms in the credit cards it makes it very difficult to forge them effectively
(Bhatla, 2003).

Notwithstanding the ultimatum by the Reserve Bank of Zimbabwe (RBZ),
instructing all financial institutions to submit cyber security policies and ensure
that they are issuing out EMV compliant cards, the March 2019 deadline lapsed
and most banks remain non-compliant (Tshili, 2019). As such, criminal syndicates are taking advantage of some Point of Sale machines and other gadgets in the market which are not EMV compliant. EMV stands for Europay, MasterCard, Visa. It is the global standard for chip-based Debit and Credit Card transactions, a joint effort between Europay, MasterCard and Visa to ensure security and global acceptance, so that MasterCard and Visa Cards can continue to be used everywhere.

**Skimming**

Skimming is fast emerging as the most popular form of credit card fraud. Most cases of counterfeit fraud involve skimming. It is a process where the actual data on a card’s magnetic strip is electronically copied onto another. Fraudsters have been found to carry pocket skimming devices, a battery-operated electronic magnetic strip reader, with which they swipe customer’s cards to get hold of customer’s card details. The fraudster does this whilst the customer is waiting for the transaction to be validated through the card terminal. The card holder will not be aware about this and it would be very difficult for him or her to know about it or detect it. In other cases, the details obtained by skimming are used to carry out fraudulent card-not-present transactions by fraudsters. Until the cardholder gets the bill he or she does not understand since there is no way of finding out about the fraud (Bhatla, 2013).

### 2.6 Challenges in curbing Card fraud

**Problems in defining card fraud**

One of the problems in countering card fraud is that there is no single definition of card fraud (Bakan, 2004). The Benefits Card fraud Inspectorate in UK say that it is, ‘the deliberate misrepresentation of circumstances or the deliberate failure to notify changes of circumstances with the intent of gaining some advantage’, while the UK Treasury says that card fraud is the ‘use of deception with the intention of obtaining advantage, avoiding an obligation or causing loss to a third party’ (NERA, 2000). It would be difficult to meaningfully apply either of these definitions to card frauds committed by MNCs, where deliberately misrepresenting circumstances or using deception to obtain advantage may be construed as normal business strategy. Landmark cases (*Dodge v. Ford Motor*
Company 170 N.W. 668 (Mich. 1919); Hutton v. West Cork Railway Co (1883) 23 Ch D 654) have determined that the ruling business ethic is that profits be maximised for the benefit of shareholders; if deception helps to maximise profits it is justified unless the deception is specifically prohibited by the law (Bakan, 2004). It seems, therefore, just as benefit card fraud is defined by what constitutes illegally deceptive behaviour for claimants, corporate card fraud must be defined by what constitutes illegally deceptive behaviour for corporations (and their agents).

Non-reporting of card fraud cases
Card fraud cases usually involve wealthy corporations and individuals who have much influence in society thereby making it difficult for anyone to report them when they commit crime. Usually in these circumstances, whistle-blowers are not protected hence people fear reporting. Political, institutional and ideological pressures contribute to the non-reporting of card fraud crimes. Insiders may be deterred from raising the alarm about card fraudulent activity, especially if it is being conducted by someone senior to themselves or by a client important to their business because of unpleasant consequences, including dismissal for breach of confidence (Robinson and Bennett, 2012).

When Sutherland first described white-collar crime, he was trying to correct the apprehension that crime was concentrated in the lower socioeconomic class and that, in fact, crime could ‘be committed by a person of respectability and high social status in the course of his occupation’ (Sutherland, 1983). Furthermore, card fraud is difficult to detect especially if it does not directly involve prejudicing another person hence such cases just go unreported. It is clear, though, that investigating card fraud is frequently an unglamorous, frustrating, unrewarding and under-appreciated arm of law enforcement.

Lack of competence
The police and the criminal justice delivery system base most of their decisions to enforce law, charge and convict a person on their own discretion. The effectiveness of these discretionary powers is highly dependent on the level of understanding of crime in question by the respective officer, availability of
requisite skills and training to manage the crime, availability of resources to see through the process of detection, investigation apprehension, and conviction (Njanike et al., 2009). Card fraudsters especially in multi-national corporates use highly sophisticated means to wire large amounts of money to offshore accounts without leaving a trace, this means detection would require high technical abilities and this is where most of the police officers fall short (Njanike et al, 2009). In Zimbabwe the police have to rely on audits by various auditing firms to detect card fraud on their behalf. Unless reported there is usually no way of telling whether card fraud was committed or not as police lack requisite resources.

**Globalization and Jurisdiction**

Globalization although it has brought so many merits to the socio-economic development of the world, it has also been used to fuel card fraudulent activities taking advantage of the limitations of legal jurisdiction and sophisticated technologies. Formerly, it was a general principle that no-one could be tried in England and Wales for an offence committed abroad unless there was a statutory provision that permitted it. It was not thought possible to prosecute criminal acts committed abroad in English and Welsh courts unless the perpetrators were British subjects and foreign subjects could not be tried in the UK for offences committed overseas (Kirk and Woodcock, 2003). These rules arise from the territorial nature of criminal law which presumed that a crime could only be committed in one place and where attempts to interfere in the jurisdiction of other states would almost certainly have been construed as an attack upon their sovereignty (Kirk and Woodcock, 2003).

While many countries today allow for extradition of criminals others still maintain that it is breach of their sovereignty. The consensus in international law is that a state does not have any obligation to surrender an alleged criminal to a foreign state, because one principle of sovereignty is that every state has legal authority over the people within its borders. No country has an extradition treaty with all countries for example; the United States lacks extradition treaties with Russia, China, and Namibia among other countries. Furthermore, even if extradition is allowable, countries like Australia, Canada and New Zealand will not allow it if
death penalty may be imposed on the suspect. However, there is now an increasing understanding that the international nature of Multi-National Corporations operations make it necessary to look beyond state borders.

2.7 Measures to improve policing card fraud

Early card fraud detection and eradication
Mclachlan (2009) states that the incidence of card fraud in recent time seems to be a rather pervasive phenomenon, and no one is in doubt about the tremendous effect and consequences that it poses to the stability of the larger economy. It is therefore recommended that more active attention is paid to early card fraud detection and eradication (Mclachlan, 2009). One way of achieving this is that police should ensure that commercial and residential premises alike ensure additional security devices are incorporated. Use of serialised documentation for institutions such as, banks, passport offices, universities among others, not only within the premises but also in the cheque books, receipts or certificates given to their numerous clients. This not only helps reduce their vulnerability to forgeries and other card fraudulent acts, but also makes early detection of such nefarious acts easy.

Conduct thorough background checks and Training
In recruiting key personnel who are to handle certain sensitive operations, it is essential that the police help corporations make concerted efforts at conducting a proper background check on the status and nature of the employee in his or her neighbourhood, as this would help them establish the probability of the employee engaging in card fraudulent activities (Rowan, 2012).

Increasing the police’ ability to detect card fraud is important. This can be achieved through a combination of internal and external modules of on the job training and off the job training exercises (Rowan, 2012).

Companies should improve employees’ conditions of service
Occupational card fraud is rampant thus companies should also advised to continuously review compensation packages to reduce the tendency for card
fraudulent behaviour by their employees (Cole, 2013). It is believed that if employees are well remunerated the incidence of card frauds will reduce. Also, favourable financial awards and recognition should be given to employees who show dexterity in identifying and preventing card fraud. Abraham Maslow in his theory of the hierarchy of needs gives a detailed guideline on essential human needs and how satisfaction of these needs boosts morale, thereby reducing deviancy.

**In-calculation of good corporate governance principles**

Bhatia (2013) recommends that sound corporate governance characterized by effective operational practices comparable to international standards, should be adopted by top management of organizations as an essential ingredient for the prevention of card fraud in the banking sector. Top management must also strive to maintain a high degree of ethical standards in the performance of their duties, in view of the fiduciary nature of their functions (Bhatia, 2013).

This is imperative as they are by law required to safeguard the assets of their institutions (Carmody, 1998). Also the internal audit department of banks should not be seen as a dumping ground for non-performing staff. Staff deployed into this department should be sufficiently qualified, properly trained and adequately experienced in all facets of banking operations.

As Carmody (1998) and Imhanlahimi (2001) have pointed out, the high level of enforcement of laws, rules and regulations begets higher goals achievement in the social system or organizations concerned. The state’s law enforcement agencies must therefore, be above board in assisting the banking institutions in the enforcement of the regulatory guidelines (which includes card fraud reduction in the banking system) for banks to operate. Carmody (1998) puts it this way; the state must be strong and hard to bring about development, in this case through early card fraud detection and eradication. The heart of this recommendation is that there should be strict specification of regulatory guidelines for banks to operate, and then strictly enforce them objectively without fear or favour through the active and unalloyed cooperation of the law enforcement agencies or institutions.
**Raise perceptions of being caught**

Hollinger and Clark (1983) found that the single most effective way to prevent theft was to raise the chances, or the employees’ perception of the chances, of getting caught: The stronger the perception that theft would be detected, the less the likelihood that the employee would engage in deviant behaviour (Robinson and Bennett, 2012).

Social control in the workplace, according to Hollinger-Clark, consists of both formal and informal social controls. The former control can be described as the internalization by the employee of the group norms of the organization; the latter, external pressures through both positive and negative sanctions. These researchers, along with a host of others, have concluded that as a general proposition informal social controls provide the best deterrent (Robinson and Bennett, 2012).

**Empirical Review**

Kunz and Wilson (2004) conducted a study on problems in policing card fraud in Toronto. Their findings revealed that policing card fraud is affected by the complexity of the crime. Card fraud continues to take new and different forms, as such, defining it has proved elusive. Wells (2012) agrees with Kunz and Wilson (2004), when he says, there is no uniform way of defining card fraud as it continues to change shape and form. Thus this study sought to investigate whether policing card fraud in Zimbabwe is affected by complexity of the crime and its chameleonic behaviour.

Van der Vijver and Terpstra (2007) conducted a study in Germany entitled, “Causation of computer card fraud”. Van der Vijver and Terpstra (2007) found that, computer card frauds are normally committed by people who have the access and opportunity to manipulate records. They also revealed and this is supported by Milner (2008) in a follow-up study, where he says computer card fraud is as a result of opportunity and greed as well as lack of robust controls. Thus, the researcher in this study sought to investigate whether the rise in card fraud cases in Zimbabwe is as a result of access, opportunity or greed.
Coleman and Moynihan (2010) conducted a study in China on “Card fraud detection”. Coleman and Moynihan (2010) concluded that card fraud is difficult to dictate firstly due to the fact that the people who commit are the people, the organization trust and have vested the power to safeguard its resources. Thus, it takes time to detect and when it is detected (particularly by employees) it may be difficult to report for fear of victimization. The National Economic Research Associates (NERA) says that card fraud is unusual in that there is significant potential for it to be undiscovered, either for a period of time or permanently (NERA, 2000). Therefore, this study sought to investigate whether lack of detection was one of the causes of increase in card fraud cases in Zimbabwe.

Kharna (2009) conducted a study in India on “Reasons of Bank Card frauds”. The aims of the study were to evaluate the various causes that are responsible for banks card frauds. Another objective was to examine the extent to which bank employees follow the various card fraud prevention measures including the ones prescribed by Reserve Bank of India. Kharna (2009), found that, a strong system of internal control and good employment practices prevent card frauds and mitigate losses. The research reveals that implementation of various internal control mechanisms are not up to the mark. The results indicate that lack of training, overburdened staff, competition, low compliance level (the degree to which procedures and prudential practices framed by Reserve bank of India to prevent card frauds are followed), are the main reasons for bank card frauds. Could it be possible that the findings raised by Kharna (2009) are the causes of card fraud in Zimbabwe?

Ernst and Young (2002), conducted a study in UK, to investigate “effects of card fraud on victims”. The finding that the majority of corporate card fraud is committed internally, by management (55%) or other employees (30%), adds a personal element that other corporate officers might find difficult to deal with (Ernst and Young, 2002). During a study into the long-term effects of card fraud on private investors, the researchers noted that the victims displayed a peculiar sense of self-blame and victimisation. There are industry victimisation’ card fraud surveys conducted by, for example, Ernst and Young, KPMG and the
Association of British Insurers (Card fraud Advisory Panel, 1999). These are valuable in terms of assessing the impact of corporate card fraud, but are flawed by their reliance upon respondents’ willingness to admit to losses.

Idor (2010) conducted a study in Nigeria entitled, “Bank Card frauds in Nigeria: Underlying Causes, Effects and Possible Remedies”. The study sought to find out the common types of bank card fraud that are frequently carried out in the banking system, the underlying causes, level of staff involvement, consequences and possible means of ameliorating the problem. The study revealed that there was an equal level of staff involvement in initiating and executing card fraud, with the concealment of card fraud coming last in their agenda. Also, among the factors hypothesized to encourage bank card fraud; the major individual based factors were greed, infidelity and poverty, while organizational factors were inadequate staffing, poor internal controls, inadequate training and poor working conditions (Idor, 2010). Thus, this study therefore, sought to investigate whether Idor (2010)’s findings would dovetail the Zimbabwean situation.

The previous research studies reviewed here give a research gap to the current study which focuses on investigating causes of increase in card fraud cases reported to CID Commercial Crime Division, Harare. The gap arises because other researchers focused in card fraud from a corporate standpoint but this study is from policing standpoint where the researcher aims to determine challenges inherent in policing card fraud and come up with solutions.

2.8 Chapter Summary

This chapter focused on literature review conceptual, theoretical and empirical review of card fraud, causes of card fraud and challenges in policing card fraud. Chapter three will focus on research methodology.
CHAPTER III

RESEARCH METHODOLOGY

3.1 Introduction
The previous chapter focussed on literature review. This chapter covered research design, population and sampling, research instruments, data collection procedures, data presentation and analysis procedures, ethical considerations and the chapter summary in relation to the increase in cases of fraud.

3.2 Research design
According to Robertson (1987), methodology is a system of rules and principles that guide scientific investigation. Research design according to Cooper and Schindler (2003) is “the plan and structure of investigation so conceived as to obtain answers to research questions”. The design of this research study is the descriptive survey defined by Best and Khan (1993) as the method that gathers data for purposes of examining the characteristics, opinions or intentions of that population.

3.2.1 Advantages of using the descriptive survey
The descriptive survey was chosen because it was the best in terms of carrying out a research which is both qualitative and quantitative. Descriptive survey allowed the researcher to quantify the number of fraud cases received by Commercial Crime Department while interviews allowed for qualitative findings to be collected based on perceptions, emotion and feelings.

Furthermore, the descriptive survey enabled the collection of data from many respondents in a short space of time and within limited resources.

3.2.1 Disadvantages of descriptive survey
The descriptive survey had its limitations in that the researcher used structured questions making it difficult to be flexible to follow through emerging issues particularly from the interviews. Moreso, with questionnaires, the researcher could not probe or seek clarification on ambiguous responses. Similarly, the researcher was not available to give clarity to the respondents.
3.3 Population
Bless and Higson (1995) define population as an aggregate of elements from which a sample can be selected. In this research study the target population referred to all the 120 police officers of CCD, 400 complainants of the year 2017 and 2018 and 180 FBC Bank employees. The target population therefore was 700. The nature of the population has implications on the sampling method in this case the population is finite.

3.4 Sample
Borg and Hall (1974) define a sample as that part of a large population that gives a representation of the entire population. According to Nachnias and Nachnias (1996), the sample size that is the best representation of the population mathematically is between 10 and 30 % of the population. Thus in this study 10 percent of the 700 target population was drawn to make up the sample which translated to 70. Considering that the population of the study is finite, it follows, therefore that this study adopts probability sampling method. Justification being that each and every observation in the population should be given an equal chance of being selected.

3 Sampling Procedure and Techniques

Sampling technique
This study adopted a stratified sampling technique and simple random sampling technique. The first technique adopted sought to determine representation of the respondents from each stratum. Justification for this approach emanates from the nature of the population which has three strata, in the form of police officers, bank employees and card fraud complainants. The following formular as suggested by Kumar (2014), s/N x n=k, where:

- S, represents size of the stratum
- N, represents the population size
- n, represents sample size;
- k, represents the stratum representation
Adopting this formular number of respondents to be included in the sample are;

<table>
<thead>
<tr>
<th></th>
<th>Stratum size</th>
<th>Sample size</th>
<th>Representation of stratum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police officers</td>
<td>120</td>
<td>70</td>
<td>12</td>
</tr>
<tr>
<td>Complainants</td>
<td>400</td>
<td>70</td>
<td>40</td>
</tr>
<tr>
<td>FBC Employees</td>
<td>180</td>
<td>70</td>
<td>18</td>
</tr>
<tr>
<td>Total</td>
<td>700</td>
<td></td>
<td>70</td>
</tr>
</tbody>
</table>

Having determined the representation from each stratum, the study went further to invoke simple random technique to choose representatives from each stratum. This technique was adopted to eliminate biasness in the selection of research participants. According to Saunders et al (2003), simple random sampling is a process of selecting a sample in such a way that all individuals in the defined population have an equal and independent chance of being selected from the stratum by codifying and randomly picking individuals.

3.5 Research Instruments

Leedy (1980) defines a research instrument as a device used to observe data beyond the physical reach of observation. According to Peil (1981) a research instrument refers to a tool or equipment used to collect data for example, questionnaires, interviews and observations. The interview and observations compliment the questionnaire hence in this study interviews and questionnaires were used to address research questions of this study. Research instruments had chosen satisfied reliability and validity. Leedy (1983) defines validity as the effectiveness of a measuring instrument in measuring what it is supposed to measure. Saunders et al (2003) is of the opinion that reliability is the degree to which data collection methods will yield consistent findings, similar observations would be made or conclusions reached by other researchers or there is transparency in how sense is made out of raw data.

3.6 Questionnaires

Leedy (1993) considers a questionnaire as the most extensively used method for accumulate primary data. Borg and Gall (1974) describe a questionnaire as a document that asks some questions from all individuals of the sample. The researcher used the
questionnaire to ask questions consisting of scaled response questions, multiple choice questions which solicit for yes/no answers and open-ended questions to all respondents. It is important to mention that the choice of the type of questions was based on the requirement for translating the recorded responses into some form that facilitates ease of analysis.

Advantages of questionnaires

Questionnaire provided a number of benefits to the researcher:-

Questionnaires covered a wide range of the matters such as attitudes, opinions, ideas, experiences and perceptions needed to meet the objective of the study. They also reached a wider range of respondents. They were also constructed to determine attitudes of individuals so that opinions of large numbers of individuals can be summarized to describe the overall attitudes of a group on a certain topic using samples.

Questionnaires also provided uniformity because of their standardized nature thereby eliminating bias, reducing errors likely to result from personal characteristics of the different respondents. Furthermore, questionnaires were impersonal, respondents answered questions on their own with very little pressure and anonymously hence ensured that responses given by respondents are freely given with less bias.

Questionnaires allowed the researcher to use open-ended questions which are adaptable to studies based on the qualitative analysis of data. With open-ended questions the researcher was able to collect data of a perceptive nature which gave a rich interpretation of data.

The questionnaire also enabled the researcher to use structured questions. The advantages were that they allowed for comparison and quantification of the results. The responses were also simple to record and score. Structured questions collect data which is easily comparable.

Disadvantages of questionnaires

Questionnaires did not give the researcher room for face to face or personal interaction with respondents as such; the researcher could not probe, seek clarification or read non-
verbal cues to determine the respondent understanding of the questions. To counter this problem, the researcher had carried out a pilot study which helped a lot to simplify language used in crafting the questions. Interviews were also carried out to mitigate any challenges faced in answering questionnaires.

Secondly the researcher did not have control over the data provided whether it was true or false and whether the questionnaires were actually responded to by the intended recipients. The researcher countered this problem by asking the sections heads to create an environment that would ensure all respondents participated freely and in person.

3.7 Interviews

While questionnaires provide more of the quantitative data, interviews are more qualitative in nature hence the reason for their simultaneous use in this research study. Haralambos and Horlbom (2006), define an interview as a face-to-face interaction whereby the respondents answer the researcher’s questions. According to Borg et al (1996), interviews consist of oral questions by interviewer and oral responses by research participants.

Advantages of interviews

Interviews were used in this study because they provide an effective and efficient method of data collection because researcher was able to probe and respondents were able to seek clarification thereby enabling correct interpretation of questions and answers. Moreover in an interview, the interviewer has more control than in other kinds of data collection instruments.

Furthermore, the researcher gained a deeper understanding of the validity of responses. Interviews are flexible and they allow appraisal of validity of the responses. More so, the interviewer had a chance to encourage respondents to be free and accurate in giving their answers; and also there was personal contact which facilitated greater validation of responses through reading of non-verbal language such as sitting positions, facial expressions, and areas emphasized.
Disadvantages of interviews

The researcher realised that interviews just like questionnaires had weaknesses. Personal interaction though its benefits outweigh demerits, posed a threat of bias as researcher’s own personal values and perceptions of interview had a temptation of interfering with objectivity. This was curbed by the use of questionnaires to complement responses from the interview.

In some instances respondents were afraid of freely expressing themselves for fear of being sold out to commanders on their weaknesses. The interviewer assured them of the anonymity of respondents’ identities and confidentiality of all responses given. Emphasis on the fact that the interview was strictly for academic purposes helped to minimise anxiety and false answers.

3.8 Pilot Study

According to Saunders et al (2003), a pilot test is a small-scale study to test a questionnaire or interview check list, to minimize the likelihood of respondents having problems in answering the questions and of data recording problems as well as to allow some assessment of the questions’ validity and reliability of the data that will be collected. In this study a preliminary analysis using the pilot test data was undertaken to ensure that the data collected will enable investigative questions of the research study to be answered. The researcher carried out a pilot study which consisted of subjects with the same attributes as the study sample to test the reliability of the questionnaires. Two (2) police officers from CCD and two (2) FBC employees were given the questionnaires to attempt to answer them. Questions from section B were revised after pilot study revealed that they did not quite understand what was expected of them. The questions were based on the research study’s objectives to ensure reliability and validity of the findings.

3.9 Data collection procedures

Researcher collected both primary and secondary data to ensure the research objectives were met. The researcher distributed all the questionnaires by hand to the respondents and gave section heads to distribute and collect on behalf of the researcher. A total of 50 questionnaires were distributed. The interviews were carried out in a private and secure
environment, with each session taking approximately ten minutes. A total of 20 interviews were carried out.

3.10 Presentation, Analysis and Interpretation of Data

Qualitative data was presented in themes under headings to cover research objectives. Quantitative data was presented in the form of tables, bar charts, and pie charts, histograms, in line with the aim and objectives of the research study.

Data analysis in this study was aimed at addressing the objectives of the study either quantitatively or qualitatively. The aim of the researcher in data analysis was to present results that are accurate, well clarified and comprehensive and easy to read hence the use of charts to present collected quantifiable data. To ensure elimination of ambiguity, the researcher gave descriptive interpretation of the information presented relating it to the previous research findings.

3.11 Ethical Considerations

Ethics, according to Saunders et al (2005) relate to questions about how we formulate and clarify our research topics, design our research questions and gain access, collect, process, store and analyse data. The researcher ensured that research ethics were adhered to by seeking authority to access data and respondents from relevant authorities. Research findings were written in a moral and responsible way in terms of being methodologically sound and morally defensible to all those who are involved.

Furthermore, the researcher also ensured that ethical issues surrounding anonymity of respondents, confidentiality of organizational secrets, impartiality, objectivity and lawfulness of the whole procedure was maintained. The research was designed in such a way that a respondent does not suffer physical harm, discomfort, pain, embarrassment, or loss of privacy. To safeguard against these, the researcher explained study benefits; explained respondent’s rights and protections and; obtained informed consent.

3.12 Summary

In this chapter, focus was on research strategy (survey), population sample size, sampling design and procedures, instruments design, data collection procedures,
presentation, analysis and interpretation. Methodological aspects involving research instruments namely; the questionnaire and interviews; their strengths and weaknesses where considered as well as issues of validity and reliability. Though there are limitations in the data collection tools used, it is apparent that they were of great help in gathering data for the purposes of this research. The next chapter will focus on data presentation and analysis in detail.

CHAPTER IV

DATA PRESENTATION, INTERPRETATION AND DISCUSSION
4.1 Introduction

Chapter three covered the research methodology. Chapter four covers data presentation, analysis, interpretation and discussion in line with research objectives which were:

➢ To establish the causes of card fraud in the banking sector.
➢ To ascertain factors impeding effective policing of card fraud in the Zimbabwe Republic Police.
➢ To establish ways of mitigating challenges in policing card fraud in the banks.
➢ To recommend on strategies to curb card fraud.

The aim of this chapter was to establish respondents’ views on common forms of card fraud, effectiveness of current strategies in preventing card fraud, challenges faced in policing and ways of improving card fraud policing.

4.2 Response rate

Table 4.1: Questionnaire distribution of response rate  

<table>
<thead>
<tr>
<th>Research instrument</th>
<th>Number administered</th>
<th>Number responded</th>
<th>% Response Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questionnaire</td>
<td>50</td>
<td>50</td>
<td>100%</td>
</tr>
<tr>
<td>Interview</td>
<td>20</td>
<td>20</td>
<td>100%</td>
</tr>
</tbody>
</table>

*Source: Primary data*

Table 4.1 indicates that fifty (50) questionnaires were distributed and all were returned thereby achieving a 100 percent response rate. Similarly twenty (20) interviews had been scheduled and all were achieved thereby achieving a 100% response rate. The research achieved a high response rate in questionnaires distribution thereby giving confidence in the results obtained. High response rate is an important indicator of survey quality. It is said to eliminate sample bias. High response rate also assures more accurate survey results.

4.3 Demographic data
The importance of demographic data in a study is that it helps the researcher breakdown overall responses based on background of respondents. This study assessed demographic data using gender, age, education, and length of service attached to CCD and at FBC.

**Respondents’ distribution by sex**

Table 4.2 Distribution of respondents by sex n=70

<table>
<thead>
<tr>
<th>Sex</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>20</td>
<td>29%</td>
</tr>
<tr>
<td>Male</td>
<td>50</td>
<td>71%</td>
</tr>
</tbody>
</table>

*Source: Primary data*

Table 4.2 above indicates that twenty (29%) respondents of this study were female while 71% were male. Data presented in Table 4.2, shows that the majority of the respondents are male while females are the minority.

The police and the banking sector are male dominated while others are female dominated based on the duties and responsibilities of the section. Similarly, card fraud affects resource owners who are also dominantly male hence the high number of males in this study as opposed to females.

**Respondents’ distribution by age**

Table 4.3: Respondents distribution by age n=70

<table>
<thead>
<tr>
<th>Age</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>21-30 years</td>
<td>19</td>
<td>27%</td>
</tr>
<tr>
<td>31-40 years</td>
<td>23</td>
<td>33%</td>
</tr>
<tr>
<td>41-50 years</td>
<td>20</td>
<td>29%</td>
</tr>
<tr>
<td>51 years and above</td>
<td>8</td>
<td>11%</td>
</tr>
</tbody>
</table>

*Source: Primary data*

Table 4.3 above indicates 27% of the respondents were aged between 21 and 30 years, while 33% were aged between 31 and 40 years, 29% were aged between 41 and 50 years and 11% were aged 51 years and above. Table 4.3 shows that
the majority of the respondents were between 41 and 50 years old while the minority were aged between 51 years and above. The respondents in the study indicate a sufficiently mature group who are expected to know much about the researcher’s area of study.

- Respondents’ distribution by education

Table 4.4: Respondents distribution by Education  

<table>
<thead>
<tr>
<th>Education</th>
<th>Number</th>
<th>Percentage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>16</td>
<td>23%</td>
</tr>
<tr>
<td>Diploma</td>
<td>28</td>
<td>40%</td>
</tr>
<tr>
<td>Degree</td>
<td>12</td>
<td>17%</td>
</tr>
<tr>
<td>Other (specify)</td>
<td>14</td>
<td>20%</td>
</tr>
</tbody>
</table>

Source: Primary data

Table 4.4 indicates that 23% of respondents are holders of certificates, 40% are holders of diplomas, 17% are holders of degrees and 20% indicated other qualifications such as Ordinary level and Advanced level.

The majority of the respondents are holders of diplomas while the minority (17%) have degrees. The respondents had sufficient educational background to competently respond to questionnaires giving meaningful contributions on general comments.
4.4 SECTION B

Commonly reported forms of fraud

Figure 4.1 Respondents views on commonly reported forms of fraud n=70

Source: Primary data

Figure 4.1 above shows the frequency of forms of fraud commonly reported at CID Commercial Crime Department. Computer fraud had a frequency of 44%, occupational fraud 78%, Insurance fraud 60%, 100% housing scam fraud and 83% card fraud. Table 4.6 indicates that the most frequently reported forms of fraud are housing scams and the least are computer fraud. It is key, to note that although card fraud is emerging in Zimbabwe, it has already overtaken other forms of fraud.

A study by Kunz and Wilson (2004) indicated that computer and insurance frauds were rife in Nigeria contrary to the Zimbabwean situation were housing scams are on the most popular forms fraud.
Card Fraud prevalence

Table 4.5: Respondents’ views on whether card fraud is increasing or not  n=70

<table>
<thead>
<tr>
<th>Respondent’s response</th>
<th>Number</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>70</td>
<td>100%</td>
</tr>
<tr>
<td>No</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Primary data

Table 4.5 shows 100% of respondents indicating that fraud is on the increase. Card fraud is on the increase thereby proving the existence of a problem in fraud policing.

Reasons for the increase in card fraud

Table 4.6 Respondents reasons for increase in card fraud  n=70

<table>
<thead>
<tr>
<th>Respondent’s response</th>
<th>Frequency</th>
<th>Percentage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low detection</td>
<td>40</td>
<td>57%</td>
</tr>
<tr>
<td>Poverty</td>
<td>60</td>
<td>86%</td>
</tr>
<tr>
<td>Greed</td>
<td>60</td>
<td>86%</td>
</tr>
</tbody>
</table>

Source: Primary data

Table 4.6 shows the respondents’ views on what is causing card fraud. 57% indicate that it was low detection; 86% showed that it was poverty and 86% indicated that it was because of greed. Based on data presented in Table 4.6, the majority of respondents indicated greed as a major reason for increase in card fraud while low detection rate was the least cause. This is in line with Donald Cressey’s fraud triangle which concludes that individuals commit fraud when there is a financial need that cannot be shared, a perceived opportunity for illicit gains and a personal rationalization of the act (Coleman, 1998).
Common perpetrators of card fraud

Figure 4.2 Respondents response on card fraud perpetrators n=70

Source: Primary data

Figure 4.2 shows that 44% of the respondents thought senior ranking employees were the common perpetrators of card fraud, while 34% indicated junior ranking employees, 72% indicated 72% and 100% indicated strangers. Data in Figure 4.3 shows that the majority of respondents felt that strangers were the common perpetrators of fraud. Data in Figure 4.3 indicates that generally everyone is a potential perpetrator of card fraud provided there is according to Cressey, a perceived opportunity, gain and a rationalization (Coleman, 1998). This is supported by Hollinger-Clark’s workplace fraud theory where he says employees steal primarily because of lack of organizational controls. When an employee perceives the chances of being caught as slim, they are likely to engage in fraud.
4.5 Current strategies being used by CCD to curb fraud

Table 4.7 Current strategies to curb card fraud  n=70

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Frequency</th>
<th>Percentage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specialized card fraud management training</td>
<td>50</td>
<td>71%</td>
</tr>
<tr>
<td>Inter-agency policing</td>
<td>28</td>
<td>40%</td>
</tr>
<tr>
<td>Financial Intelligence units</td>
<td>20</td>
<td>29%</td>
</tr>
<tr>
<td>Community policing initiatives</td>
<td>68</td>
<td>97%</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Primary data

Table 4.7 shows that 71% of respondents indicate that specialized card fraud management training was one of the current strategies being used by CCD to curb fraud, 40% indicated inter-agency policing and 97% indicated also community policing initiatives. Data in figure 4.7 shows that specialized fraud management training and community policing initiatives are the commonly known and used fraud management strategies. This is however not consistent with ZIMPOD Vision 2020 which stipulates that these strategies as one broad strategy whereby use of one or two without the other will result in poor performance.

Assessment of whether strategies are effective in curbing card fraud

Figure 4.3 Respondents’ view on effectiveness of current strategies  n=70

Source: Primary data
Figure 4.3 indicates the respondents’ perspective of the effectiveness of the current strategies used by CCD in dealing with fraud. 16% said ‘Yes’ they were effective while 17% said they were ‘somewhat effective’. The majority of respondents (60%) indicated that the strategies were not effective. This means therefore that there is need to carry out some reformation in the study.

4.6 Operational challenges in policing card fraud

Table 4.8 Respondents’ views on operational challenges n=70

<table>
<thead>
<tr>
<th>Respondent’s response</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity of crime</td>
<td>70</td>
<td>100%</td>
</tr>
<tr>
<td>Non-reporting of crime</td>
<td>8</td>
<td>11%</td>
</tr>
<tr>
<td>Incompetency of police</td>
<td>24</td>
<td>34%</td>
</tr>
<tr>
<td>Technology and jurisdiction</td>
<td>58</td>
<td>83%</td>
</tr>
<tr>
<td>Other</td>
<td>23</td>
<td>33%</td>
</tr>
</tbody>
</table>

Source: Primary data

Table 4.8 above shows the frequency of operational challenges in policing card fraud. 100% of respondents indicated that complexity of the crime was a major operational challenge while 11% indicated non-reporting of crime, 83% sighted technology and jurisdiction and other challenges had a frequency rate of 33%, 34% cited police incompetence. The majority of the respondents indicated that complexity of crime was a major operational challenge while non-reporting was the least. Other challenges like resources shortages were also mentioned. This in line with Nera (2000)’s assertion that there is no single definition of fraud. Fraud continues to evolve both on the street and in the organizations. It is becoming more complex and difficult to identify or investigate.
Causes of ineffectiveness of legislation in managing card fraud

Table 4.9 Respondents views on effects of legislation on fraud management

<table>
<thead>
<tr>
<th>Respondent’s response</th>
<th>Frequency</th>
<th>Percentage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some pieces of legislation are ambiguous</td>
<td>58</td>
<td>83%</td>
</tr>
<tr>
<td>Legislation does not cover all forms of card fraud</td>
<td>70</td>
<td>100%</td>
</tr>
<tr>
<td>Legislation is difficult to enforce</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Primary data

Table 4.9 above shows the respondents’ views of how legislation affects management of card fraud. 83% of the respondents indicated that some pieces of legislation are ambiguous while 100% indicated that the available legislation does not cover all forms of fraud. None of the respondents indicated that the legislation is difficult to enforce but the issues raised were that it does not cover all forms of fraud and that some of the pieces of the legislation are ambiguous. This is in line with Kunz and Wilson (2004) who posit that fraud is complex, continues to take different forms; as such defining it has proved elusive. Without definition of an act perceived to constitute fraud, a perpetrator can get off on technical grounds.
4.7 Recommendations

Table 4.10 Respondents views on ways to improve card fraud management
n=70

<table>
<thead>
<tr>
<th>Respondent’s response</th>
<th>Frequency</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intensive co-operation with the public</td>
<td>70</td>
<td>100%</td>
</tr>
<tr>
<td>Protection of whistle blowers</td>
<td>70</td>
<td>100%</td>
</tr>
<tr>
<td>Continued upgrading of members’ skills</td>
<td>70</td>
<td>100%</td>
</tr>
<tr>
<td>Forge regional and international anti-fraud alliances</td>
<td>47</td>
<td>67%</td>
</tr>
<tr>
<td>Other</td>
<td>50</td>
<td>72%</td>
</tr>
</tbody>
</table>

Source: Primary data

Table 4.10 above shows the respondents suggestions of what can be done to improve management of card fraud cases. 100% of respondents indicated that intensive co-operation with the public, protection of whistle blowers, and continued upgrading of members’ skills are measure that can improve card fraud management. 67% indicated that, forging regional and international anti-fraud alliances also improves card fraud management while 72% endorsed various other measures. All respondents indicated that intensive co-operation with the public, protection of whistle blowers, and continued upgrading of members’ skills are key towards the improvement of the fraud policing. The results obtained in Table 4.10 indicate that a holistic approach should be adopted to engage all sectors involved in the successful implementation of fraud management strategies.

4.8 Summary

This chapter looked at data presentation, analysis, interpretation and discussion from findings on the research topic, a study into the increase of card fraud. The aim of the study was to investigate the causes of card fraud in Harare. The study also aimed to establish operational challenges in policing card fraud and ways that can help policing, thus reducing card fraud. The next chapter will look at summary of major findings, conclusions and recommendations.
CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The previous chapter covered data presentation, analysis, interpretation and discussion. This chapter covers major findings, conclusions, recommendations and recommendations for future studies. The study was meant to find out why card fraud is on the increase by establishing operational challenges faced in policing it and thus identify ways that can help reduce the crime of card fraud.

5.2 Summary of the study

This research study was organised into five chapters. Chapter one focused on the problem and its setting. In this chapter, the researcher covered background of the study, statement of the problem, research objectives, research questions, assumptions of the study, scope of the study that is., delimitations and limitations, definition of key terms and project outline.

Chapter two, covered literature review. In this chapter the researcher outlined the theoretical review covering research objectives which were (1) To find out the forms of card fraud being committed (2) To establish the effectiveness of the strategies currently being used by the police in policing card fraud and (3) To ascertain operational challenges faced by the police in policing crimes of card fraud. The researcher also covered empirical review of previous similar studies.

Chapter three covered research methodology. The researcher highlighted the research approach used in the study, the research design, population and sample size, sampling technique and procedure, research instruments, pilot study, data collection procedures, ethical considerations, validity, reliability and study limitations.

Chapter four covered data presentation, analysis, discussion and recommendations. The chapter sought to answer the research questions from the respondents with the aim of explaining why card fraud was on the increase, the
operational challenges in policing card fraud and identifying areas of improvement.

Chapter five, covered summary of the study, summary of the major research findings, conclusions and recommendations. The researcher also highlighted areas of further study.

5.3 Summary of research findings

The research findings reveal that the crime of card fraud is on the increase. Housing scams are the most prevalent form of fraud commonly reported in Harare as supported by the 100% indication from study respondents while computer card fraud, insurance fraud and occupational fraud also form commonly reported crimes of card fraud.

5.3.1 Causes of card fraud

From the research findings, it was established that:

- Most prevalent cause of card fraud is failure to protect card information by the respective cardholders, especially the unnecessary disclosure of the PIN, during transactions.

- Liquidity crunch and rampant use of plastic money without any substitute transacting method, coupled with inadequate security features on the credit cards creates vulnerability and appetite for card fraud.

- Failure to protect Personal Identification Number (PIN) of the cardholder during transaction process making it possible for the fraudsters to access it through either video recording or eavesdropping during the transaction, after which a replica card is produced and used simultaneously with the original one.

- Bank chip and pin cards allows for both chip and magnetic stripe transactions, as first instant transaction modes interchangeable. In other words the merchant, whether EMV compliant or not, chooses which slot to use on the POS without any failure. Therefore, a chip and pin card
reproduced on magnetic stripe can be used at first instance on a non-EMV compliant POS terminal after being reconfigured to a magnetic stripe.

- The same authentic card number would be maintained on both fraudulent and genuine transactions, where mostly genuine transactions would be identified as chip and pin, whilst fraudulent ones would be magnetic stripe driven. (*For illustration purposes, refer to attached document marked appendix 3, depicting an FBC Chip and Pin card cloned on a BancABC debit card.*)

- Organised criminal syndicates employing services of lowly paid Point of Sale merchant operators, who in turn assist in harvesting card information and share it with the card cloners for an undue reward.

- Ignorance on the part of card holders being taken advantage by fraudsters who claim to be bank employees and portray to register them on mobile banking platforms. Thus, a One Time Password (OTP) is sent to the unsuspecting cardholder who then divulges card credentials to the fraudsters.

5.3.2 Factors impeding effective policing of card fraud

From the research findings, it was established that;

- Card fraudsters operate in organised syndicates, with specific specialised roles to be performed by each member. Anonymity is associated with membership as role players usually do not link or know each other; the person doing the transaction will just be a front with no knowledge of the origins of the fraudulent card.

- Criminals are in possession of harvested card production data and configurations of different bank cards sequence and that information is within their domain. That is the information they are using to manufacture their cloned card without any problems.
➢ All what the criminals require is the full card number and pin, such information can be accessed as the customer transacts, mainly by means of clandestine video recording. This modus makes it very difficult to detect the exact point of cloning or where the card would have been compromised.

➢ The strict secrecy associated with organized criminal syndicates makes it difficult to get to the real culprits.

➢ High literacy rate, vast computer knowledge on the part of the card fraudsters and redundancy of skilled graduate youths, applying their skills taking advantage of low detection rate due to lack of adequate police training and investigative skills.

➢ CCD as a department does not only deal with card fraud cases but are faced with other forms of fraud such as computer fraud, occupational fraud, insurance fraud as well as housing scam fraud cases which compete for the same attention with card fraud, thereby making specialisation impossible.

➢ Non-compliance on the part of financial institutions by not deploying EMV compliant machines on the market which are able to detect manipulated or cloned credit cards.

➢ Inability by the banks to have in place adequate monitoring systems to detect duplicate card transactions through geographical location identification, especially where a duplicate card is used in a different locality.

➢ Complexity of card fraud, non-reporting of crime, ever changing technology and jurisdiction coupled with it being borderless inhibits detection.
- Failure by merchants to detect or distinguish the authenticity of the card presented during a transaction.

5.3.3 **Measures that can improve policing card fraud**

From the research findings, it was established that:

- There is need for training of merchants and shop attendants on ways of detecting a fraudulent card as a joint effort by the banks and the police.

- Awareness campaigns and workshops aimed at enlightening the public on the scourge of card fraud.

- Intelligence led policing initiatives and concentrated patrols on most areas prone to card fraud purchases, to improve disruption and early detection.

- Encourage merchants to install closed circuit television recorders to be used as an aid and fall back during investigations to assist in the identity of the card fraudsters.

5.3.4 **Strategies that can be used to curb card fraud**

From the research findings, it was equally established that:

- Dealing with card fraud is not a once off event but a process which require both short term and long term strategies, aimed at detecting any reconfigurations done on the card sequence not emanating from the bank system.

- Banks to be compliant with the regulatory requirements by deploying EMV compliant Point of Sale machines as a means to eliminate all fraudulent cards.

- All merchant POS terminal require to be interrogated to Chip Reader functionalities and disown any fall back to magnetic stripe.
Banks to equip customers with the approval and authorisation of all card related transactions through tokenisation by directing notification of any attempted purchase to the account holder mobile number for approval and authorisation.

Banks to come up with intelligence mechanism tools to detect any unfamiliar transaction patterns from individual accounts as well as ability to detect simultaneous transactions on different geographic locations.

Banks to have in place intelligent tools to detect irregular transaction patterns and constant POS related balance enquiries.

Benchmarking with other jurisdictions as well as specialized card fraud management training, inter-agency policing and community policing initiatives are the most ideal strategies to be used by CCD in fighting the crime.

Regular interface or interactions between the CCD representatives and the Banks Security Managers, during Inter-Bank Security Liaison meetings appeared to be complimentary effort. The strategies are somewhat effective based on the 61% of the respondents’ views.

Intensive co-operation with the public, protection of whistle-blowers and continued upgrading of investigators’ skills, are the main strategies that could work to prevent card fraud.

There is need to expand card fraud knowledge to all police officers during recruit training.

5.4 Conclusions
The researcher on this objective concludes that the current strategies being used by the Zimbabwe Republic Police were said to be somewhat effective by the majority of respondents according to data presented in Chapter 4.
The current strategies being used by the ZRP were identified as specialized card fraud management training, inter-agency policing, financial intelligence units and community policing initiatives. The majority of the respondents indicated that specialized card fraud management training and community initiatives were the commonly used strategies. That is to say, 70% of the respondents indicated that these strategies were somewhat effective, 30% said they were effective.

Effectiveness of a strategy is measured by its ability to satisfy the objective upon which it was put in place, however, in this survey all respondents indicated that the card fraud was on the increase implying that the strategies put in place are not effective in combating card fraud.

Furthermore, the fact that financial intelligence units are not being used as a matter of ignorance or lack of knowledge proves that the police are not taking a proactive role in policing card fraud. Financial intelligence units aim at crime surveillance and detection which help expose all planned criminal acts before they occur or at least when they are occurring imminently.

In response to the challenges faced by police in dealing with card fraud, it is submitted that the majority of respondents highlighted shortage of resources as their major operational challenge. All respondents sighted complexity of the crime as the major operational challenge. Card fraud continues to change forms every time and in most cases the police adopts a reactive strategy rather than proactive.

Respondents also indicated non-reporting as another operational challenge because, the police work with reported crimes without which it is futile to think the police will prophecy about card fraudsters pouncing on certain individuals or organizations. However, the non-reporting is mainly not deliberate but the fact that card fraud may take time to be discovered and when it is discovered usually the perpetrator would be long gone such that little or nothing is recovered.

Technology and jurisdiction plays a significant role in fuelling card fraud. The advent of computer and internet technology is the commonly used modus
operandi by card fraudsters to swindle money from unsuspecting victims. With technology, one can commit card fraud in Zimbabwe from any part of the world. Tracing the card fraudster then becomes a tall task and a fruitless one for that matter. Card fraudsters create bogus websites imitating real ones and those who fail to notice it can transact with card fraudsters only to realise it after failure to receive the goods or service sought.

Other operational challenges were shortage of resources such as travelling and subsistence allowances, computers, and skilled manpower. At the same time there is tendency for interference by other senior members in the handling cases of card fraud instead of support. This then disempowers members from carrying out effective and objective investigations.

Legislation gap and inadequate punishment of card fraud offenders renders management of card fraud difficult, considering that the penal provision in the Section 167 of the Criminal Law Codification and Reform Act, Chapter 9:27 trivialises the criminality of card fraud, with the convicted criminals being sentenced to a fine or period not exceeding three years. This is in direct contrast to the penalty prescribed on fraud by Section 136 of the same Act, which calls for a conviction of up to 35 years imprisonment.

### 5.5 Recommendations

The researcher recommends that the criminal justice system must collaborate with the legislature to review and revise the current sentencing of card fraudsters to ensure that mandatory deterrent sentences are passed onto card fraud perpetrators similar to punishments prescribed in stock-theft and rape cases. Current sentencing is not congruent with the amount of losses involved in the crime.

Furthermore, members of the Commercial Crime Department must be accorded opportunity to continue upgrading their skills, to effectively deal with card fraud considering the complexity of the crime and continued change in form of card fraud taking place. The technological vice adds on to the need for continuous
training. Both Banks and Card fraud investigators must continually research on the new forms of card fraud and conscientise the public through awareness campaigns.

It is also not sufficient to train only the police and bank officials but also all members of the criminal justice delivery system such as public prosecutor as they sometimes contribute to loss of cases in court due to inability to bring out the essential elements of card fraud.

Another major concern by members of the Commercial Crime Department was shortage of resources and skilled manpower. The members were overwhelmed with work overload. However, at the same time they did not have sufficient resources to deal with it. Therefore, the police organization is encouraged to increase the skilled manpower and resource allocation to this section as well as adequate incentives to counter corrupt tendencies.

5.6 Recommendations for future research

There are a number of areas that would make good future study areas such as the role of public prosecutors or courts in card fraud management. Another area is to look at the training given to the Commercial Crime Department, to determine its effectiveness in equipping police officers to proactively police crimes of card fraud.
References


QUESTIONNAIRE: INTRODUCTORY LETTER

Introduction
I, Ndabezinhle Moyo, am a student at the Bindura University of Science Education studying for a Bachelor of Business Administration in Police and Security Studies. As a requirement for the completion of the diploma program, students are required to carry out a research project on a problem of their choice subject to university authorities’ approval. As such I am undertaking a research entitled “Challenges in curbing card fraud in banks. A case of FBC bank from January 2017 to December 2018.”

You are therefore kindly requested to assist in the research by completing the questionnaire fully and as truthfully as you can. All the information you provide will be used solely for the purpose of this study and will be treated with utmost confidentiality. Your cooperation in this regard will be greatly appreciated.

INSTRUCTIONS

- Please answer all questions fully and honestly.
- Where boxes are provided indicate your answer by ticking [✓] in the appropriate box.
- Do no write your name, address nor any identification particulars anywhere on the questionnaire.
QUESTIONNAIRE FOR CCD SECTION AND FBC BANK EMPLOYEES

SECTION A: PERSONAL DETAILS

1. What is your gender?
   a. Male       [   ]
   b. Female     [   ]

2. Indicate your age group?
   a. 21-30 years       [   ]
   b. 31-40 years       [   ]
   c. 41-50 years       [   ]
   d. 51 years and above [   ]

3. What is your highest level of education?
   a. Certificate level     [   ]
   b. Diploma level         [   ]
   c. Degree                [   ]
   d. Other(specify) .................................................................

SECTION B: ESTABLISHMENT OF THE PROBLEM

1. What are the commonly reported forms of card fraud?
   .........................................................................................
   .........................................................................................
   .........................................................................................

2. In your opinion, would you say card fraud is on the rise?
   .........................................................................................
   .........................................................................................

3. What would you say are the reasons for the increase in card fraud?
   .........................................................................................
   .........................................................................................
   .........................................................................................
4. Who are the common perpetrators of card fraud and what is their target group?

5. What are the current strategies being used by CCD Fraud to curb card fraud?

6. In your opinion, are these strategies effective in curbing card fraud?

7. What are the operational challenges faced by the police in policing card fraud?

8. How does legislation affect management of card fraud?

9. In your opinion what can be done to improve the effectiveness of CCD in curbing crime?

Thank you for your co-operation.
INTERVIEW GUIDE FOR COMPLAINANTS

1. How old are you?
2. What is your highest level of education?
3. How did you discover you were a victim of card fraud?
4. In your opinion, how did you fall victim to card fraud?
5. Based on your answer to (4) above, what would you do to avoid falling prey in future?
6. Were you able to identify the point when your card was compromised?
7. Who are the common perpetrators of card fraud and their target area?
8. Where you satisfied in the manner the bank and police investigators handled your case? If not, what would you recommend for future investigations?
9. In your opinion what can be done to improve the effectiveness of CCD Section in curbing crime?

Thank you for your co-operation.