



ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS & ECONOMICS
DEPARTMENT OF ACCOUNTING & FINANCE
(GRADUATE PROGRAM)

**Current Practices, Challenges and Prospects of Using Credit
Cards as a Payment Method: The Case of Ethiopian Airlines
Enterprise**

By:

Temesgen Getaye

June 2015

Addis Ababa

ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS & ECONOMICS
DEPARTMENT OF ACCOUNTING & FINANCE
(GRADUATE PROGRAM)

**Current Practices, Challenges and Prospects of Using Credit
Cards as a Payment Method: The Case of Ethiopian Airlines
Enterprise**

*A Thesis Submitted to The Department of Accounting & Finance, College of
Business & Economics of Addis Ababa University in Partial Fulfilment of
the Requirements for the Degree of Master of Science in Accounting &
Finance*

By:

Temesgen Getaye

Advisor:

Asmare Emerie (PhD)

June 2015

ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS & ECONOMICS
DEPARTMENT OF ACCOUNTING & FINANCE
(GRADUATE PROGRAM)

**Current Practices, Challenges and Prospects of Using Credit
Cards as a Payment Method: The Case of Ethiopian Airlines
Enterprise**

By:
Temesgen Getaye

Approved by the Board of Examiners:

Dr. Asmare Emerie (Advisor)

Signature

Dr. Samuel Kifle (Examiner)

Signature

Dr. Habtamu Birhanu (Examiner)

Signature

DECLARATION

I, Temesgen Getaye, declare that this research, titled “Current Practices, Challenges and Prospects of using credit Cards as a Payment Method-The Case of Ethiopian Airlines” is done with my own effort. I have produced it independently except for the guidance and suggestions of my research advisor, Dr. Asmare Emerie. I assure that this study has not been submitted for any scholarly award in this or any other university.

Temesgen Getaye
Researcher

CERTIFICATE

This is to certify that student Temesgen Getaye has carried out his research work on the topic entitled “Current Practices, Challenges and Prospects of using credit Cards as a Payment Method-The Case of Ethiopian Airlines” under my supervision. This work is original in nature and it is appropriate for submission for the partial fulfilment of the requirements for Master of Science in Accounting & Finance. Certified further, that to the best of my knowledge the work reported herein doesn’t form part of any other project report or dissertation on the bases of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Asmare Emerie (PhD)

Assistant Professor of Accounting/Business Information Systems

Associate Dean for Research and Technology Transfer

College of Business and Economics,

Addis Ababa University

Addis Ababa, Ethiopia

Abstract

This research paper examined the current practices, challenges, and prospects of using credit cards as a payment method by Ethiopian Airlines and it is done by adopting concurrent mixed research approach. Qualitative methods were employed by means of interviews and review of related documents while quantitative methods were used through survey of sales agents, area managers, officers and senior managers on the area. A total of 65 questionnaires were distributed to officers and managers and 47 were collected and 6 interviews were conducted with directors and managers of the airline and that of merchant banks.

The main findings of the study were that the internal control systems of the airline are not adequate enough to prevent card frauds and mitigate the credit card financial risk. Adequate and recurrent trainings for operational and back office staff on credit card acceptance and fraud prevention and having well-organized credit card desk with skilled and sufficient man power are the main critical success factors that are not either in existence or are not effective.

Management of the airline therefore, need to take immediate corrective action to the increasing threat of card fraud by means of provision of awareness and recurrent training for operational and back office staff; implementing the latest fraud screening and fraud prevention tools in all of the airlines' sales channels; establish well-organized credit card desk with well trained and sufficient staff; establish clear policies and procedures with clear assignment of responsibilities among operational and support staff; and ensure that there is seamless and integrated system.

Key words: *Card payment industry; chargeback, card fraud, payment method, merchant, issuing bank, card schemes.*

Acknowledgements

First and foremost, I would like to acknowledge the son of Kidanemiheret- the Wholy Savior for blessing me with the ability and guidance to succeed in every aspect of my life. My heartiest thanks goes to my advisor **Dr. Asmare Emerie** for his considerable contribution in directing me on this thesis and for his invaluable guidance, encouragement and support of various kinds through some difficult times. Without him this journey would never have reached this destination.

My warmest thanks goes to my lovely wife Yezab Teshome (Mitu) whose endless encouragement, moral and support were the sources of inspiration to me, during my entire post-graduate academic career, including the period I was pursuing in this MSc in Accounting & Finance and by filling the gap and balancing my study-work-daily life. In fact I owe my life as Manager Cash & Credit Management in a glooming and growing airline, as a father of two boys and as a student of ACCA and MSc to Yezab's ability to do what I totally couldn't.

My special thanks goes to Ashna Bhawa and Cynthia Zijlstra of WorldPay Limited for their priceless material and morale support and for providing constructive feedback on my thesis from the beginning to the end. I am also highly indebted to the staff members of Ethiopian Airlines, WorldPay Limited, Euroline, and AMEX especially, Vera Trunina, Andrew Glencross, Hakan Dahlsten, Laeke Tadesse, Surafel Worku, Yoseph Getachew, Etsegenet Fikre, Kalkidan Endrias, Abraham Zerihun, and others for their kind assistance in many ways.

Finally, I want to say thank you to all my classmates especially, Fikre Menta, Tadesse Kebede, Tesfaye Alemayehu and Tesfaye Tefera for all their support from the beginning to the end of this MSc programme.

Table of contents	Page
Abstract.....	i
Acknowledgements	ii
Table of contents	iii
List of tables	vi
List of figures	vii
Acronyms	viii
Chapter One: Introduction	1
1.1. Background of The Study	1
1.2. Statement of The Problem	3
1.3. Research Questions	6
1.4. Objectives of the study	6
1.4.1. General objective.....	6
1.4.2. Specific objectives.....	6
1.5. Significance of the study.....	7
1.6. Scope of the study.....	8
1.7. Limitations of the study	8
1.8. Organization of the paper.....	8
Chapter Two: Review of Related Literature.....	9
2.1. Introduction.....	9
2.2. Airline distribution and factors affecting distribution strategy.....	10
2.3. Payment methods used in the airline industry	12
2.4. Selecting appropriate payment method(s)	12
2.5. Credit Card Transaction Processing Flows.....	13

2.5.1.	Who does what to make a payment happen?.....	14
2.5.2.	Key Functions.....	16
2.6.	Types of credit card transactions	21
2.6.1.	Card-present transactions	21
2.6.2.	Card- Not- Present Transactions (CNP)	21
2.7.	Credit Card Features and Security Elements	22
2.8.	Chargeback and chargeback prevention	23
2.8.1.	Why chargebacks occur.....	23
2.8.2.	Responding to chargebacks	25
2.8.3.	How to minimize chargebacks	26
2.9.	The Fraud Management Strategies	29
2.9.1.	Common Fraud Schemes or techniques	29
2.9.2.	Impact of Credit card frauds.....	33
2.9.3.	Fraud prevention and management	33
2.10.	Internal Control Framework.....	37
2.10.1.	Board and Management Supervision.....	38
2.10.2.	Policies and procedures	39
2.11.	Summary and knowledge gap	40
Chapter Three: Research Design		42
3.1.	Strategies of Inquiry.....	43
3.2.	Research Methods.....	44
3.2.1.	Questionnaires	44
3.2.2.	Interviews	45
3.3.	Survey Design.....	45

3.4.	Sample Design	46
3.5.	Data Analysis	47
Chapter Four: Data Analysis and Interpretation of Results.....		48
4.1.	General background of Ethiopian Airlines	48
4.1.1.	Ethiopian Airlines Distribution Channels	49
4.1.2.	Payment methods used by Ethiopian Airlines	50
4.1.3.	Parties involved in Ethiopian Airlines'' credit card sales processes	52
4.1.4.	Card present versus CNP transactions in the case of Ethiopian Airlines	53
4.2.	Data analysis and interpretations	53
4.2.1.	Background information.....	54
4.2.2.	Card acceptance and authorization practices.....	56
4.2.3.	Awareness of the PCI and Card Schemes'' standards	60
4.2.4.	Fraud prevention and management	62
4.2.5.	Effectiveness of internal control systems of the airline.....	72
Chapter Five: Summary of findings, Conclusion and Recommendation		80
5.1.	Summary of findings	80
5.2.	Conclusion	85
5.3.	Recommendation	89
6.	Bibliography	Error! Bookmark not defined.
7.	Annexes	100
7.1.	Annex I: Questionnaire	101
7.2.	Annex II: Interview	111
7.3.	Annex III: Questionnaire results	113

List of tables

Table 1: Methods of Credit Card Fraud and their percentage of occurrence.....	30
Table 2: Sample size design.....	46
Table 3: Classification of respondents by education level.....	54
Table 4: Current position and year of experience of respondents.....	55
Table 5: Request the issuing bank for authentication of the card.....	56
Table 6: Obtain valid approval code from the issuing bank.....	57
Table 7: Completion of UCCCF by customers.....	58
Table 8: Agents use less of key entry.....	59
Table 9: Awareness of rules, regulations and standards.....	61
Table 10: Descriptive statistics for fraud prevention policies, procedures, tools.....	64
Table 11: Fraud rates by geography of card issuers (card issuing country).....	67
Table 12: Card fraud count by location of card issuing banks.....	67
Table 13: Comparison of % of card fraud for CNP transactions by of sales channel.....	69
Table 14: Gross sales and fraudulent trasactions count for the years 2007 to 2014.....	70
Table 15: Existing and effectiveness of internal control systems.....	75
Table 16: Overall ET's internal control system rating.....	79

List of figures

Figure 1: Diagramatic descreption of credit card processing.....	19
Figure 2: Checking card features.....	23
Figure 3: The Chargeback Cycle	24
Figure 4: Percentage of credit card sales by card type	51
Figure 5: Growth of credit card sales over the last five years.....	52
Figure 6: Comparison of Card Fraud Rates for Q4 (Oct to Dec) of the Year 2014.....	65
Figure 7: Histograms for volume of card frauds by sales channels.....	69
Figure 8: Trend of fraudulent transaction.....	71
Figure 9: Line chart showing trend of fraud rates over the last eight months.....	72
Figure 10: Histogram on ET's management knowledge of the cost of card fraud.....	77
Figure 11: Airline industry comparison of fraud to gross sales ratio.....	83
Figure 12: Recommended payment team structure.....	93
Figure 13: Programme flowchart of fraud detection system.....	95

Acronyms

ACH	Automated Clearing House
AMEX	American Express
AVS	Address Verification Service
ATO	Airport Ticket Office
ATM	Automated Teller Machine
ARC	Airline Reporting Corporation
APM	Alternative Payment Methods
CNP	Card Not Present
CVV/CVV2	Card Verification Values
CCCF	Credit Card Charge Form
CTO	City Ticket Office
CUP	China Union Pay
DCC	Dynamic Currency Conversion
EAL/ET	Ethiopian Airlines
GDS	Global Distribution System
GSA	General Sales Agents
IATA	International Airline Transport Association
MSC	Merchant Service Charge
MOTO	Mail Order Telephon Order
PCI	Payment Card Industry
PCI SSC	Payment Card Industry Security Standard Council
PIN	Personal Identification Number
PSP	Payment Service Provider
POS	Point of Sale Terminal
RBS	Royal bank of Scotland
UATP	Universal Air Travel Plan
UCCCF	Universal Credit Card Charge Form
VbV	Verified by Visa

Chapter One: Introduction

1.1. Background of The Study

The business environment has experienced rapid and revolutionary change where information and communication technologies are the major factors catalyzing this change. The rapid growth of online commerce presents new opportunities and new challenges for companies. With business-to-consumer online commerce projected to grow, the Internet is set to become a major selling channel for the retail sector; however, doing business over the Internet exposes merchants to a much greater risk of losses due to fraud. Because of the liability policies for card-not-present transactions and because of the anonymity, reach and speed that Internet provides for fraudsters, risk management and fraud prevention have become necessary components of every e-commerce infrastructure (ClearCommerce Corporation, 2001).

These changes in the business environment in recent years have caused changes to the way organizations do their businesses. Increase in global competition; advances in information technologies, the Internet, sophisticated demands of customers; e-commerce; and changes in the social, political, and cultural environment of business all have their contribution to this change (Blocher, 2010). The increasing competitiveness of the global business environment means that firms increasingly need to search for new ways of doing business and to adopt emerging technologies (Earnst & Young, 2011). Perhaps the most fundamental of all such business changes in recent years has been the increasing use of information technology, the Internet, and performance management systems (Blocher, 2010).

The exchange of goods and services has always been a central part of society. Coins and bills support this exchange and go back as far as 3000 B.C. in Mesopotamia. However, it is not always convenient to carry money around to pay for what you need, especially for larger value purchases or when travelling. If you can't pay immediately though, how do

you get a potential merchant to trust you and hand over the items or services, you want and in return for a promise to be paid later? It was this need, the ability to have access to your funds at a distance, which drove the development of the payment systems that we have today (Helldorff, 2014).

Credit Card Fraud is one of the biggest threats to business establishments today. However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of modus operandi to commit fraud. The fraud landscape has never been more complex for merchants than this time. The internationalization of markets and evolution of purchase channels has opened the door to both revenue opportunities and greater fraud risk. Companies therefore, need a holistic payment strategy that enables them to attract customers and increase their revenue but at the same time enable them to mitigate their fraud losses.

Researches show that merchants are not giving appropriate attention to revenue losses due to card frauds. According to IATA's training manual (2009), the Royal Bank of Scotland spoke to 1,000 customers and 110 companies to find out best payment solutions. This research revealed that payment solutions are way down the pecking order of factors perceived to contribute to a company's success-well below service, price and quality of product. Yet almost half of the businesses surveyed admitted that upgrading their card payment solutions increased company profitability. According to this research one in five businesses reported an increase in profitability of between 25% and 50% following improvements to payment systems, and some claimed even greater profit growth, although the average increase in profitability according to the RBS survey, was 18%. This means taking appropriate improvement to the payment methods and to their internal controls, would lead merchants to less fraud losses and increase their customers' confidence.

1.2. Statement of The Problem

In order to reach new customers and increase sales, businesses must offer their customers the opportunity to pay in a most convenient way for them. The risks, costs and implications of these payment methods may be significant and in some cases they may tie up much needed capital. On top of this there are more partners to deal with, more players and service companies emerging on the market place, compliance issues, reporting and reconciliation requirements, all in a multi-currency environment where service and reliability are crucial (Lyon, 2008). The processing of payments and selection of payment methods is no longer a commodity issue, it is strategic. Tactical decisions do not stand the test of time and decisions with respect to payment processing need to be long term. Companies therefore, need a strategy for their payment processing (Lyon, 2008).

As the world moves closer into becoming a global cashless society, fraud also evolves into more sophisticated forms. In the past few years, credit card fraud has been one of the most sophisticated crimes in the world. Various prevention initiatives have been employed to prevent this offence and yet global payments fraud statistics suggest that more must be done to address the problem. Understanding the nature of fraud and fraud prevention may help decision makers in addressing these issues (Yogi, 2011).

Credit card fraud has been a world-wide problem for years and become a healthy and growing means of stealing billions of dollars from credit card companies, merchants and consumers (Sheridon, 2008). However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of modus operandi to commit fraud (Bhatla, 2003). Increasingly, the card not present scenario poses a greater threat as the merchant (the web site) is no longer protected with the advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the “physical world” checks necessary to detect who is at the other end of the transaction (Bhatla, 2003).

In his journal of “Building our defence against credit card fraud (Journal of Money Laundering Control)”, Yogi (2011) analyzed the trends in credit card fraud prevention in the USA, the UK, Australia and Indonesia, particularly over the period 2003 to 2007, with special focus on the fraud prevention practices in the payments systems. His study provides insights into the nature of credit card fraud, as well as a framework for designing a sound credit card fraud prevention strategy in a country’s payments system. The study also establishes that a common approach in preventing credit card fraud is reducing offenders’ opportunities to commit their offences, which often require significant amount of resources and thus sound strategy needs to be properly formulated and executed.

In his hand book of “Airline Payments”, Thomas Helldorff (2014) stated that processing payments is governed by several layers of laws, rules, standards, and compliancy regulations. The first of these layered rules and regulations is that set by the card schemes that govern all the participants of the payment transactions. The airline industry has also its own rules and standards around handling payments. Payment methods in the airline industry are standardized by IATA rules (Helldorff, 2014).

Detection and prevention of fraud is an extremely important form of risk management in the credit card industry. According to UATP’s (2014) report “The cost of accepting payments” fraud costs the airline industry close to USD 2 billion annually and approximately USD 2.4 million per airline on average. The card payment industry losses close to one billion dollars a year from fraud. These are losses only to the airline industry and don’t include losses to merchants in other industries, to card issuing companies and other stakeholders in the card payment industry. Dara and Gundemoni (2006) stated that the losses associated with these attacks has risen drastically over the past couple of years, and counterfeit fraud has now been overtaken as the most costly type of card fraud by a newer method, that of CNP fraud.

The card payment industry in Ethiopia is still at its infant stage and a vast majority of people still have to carry bags of money to travel across cities, towns and villages in the

country to trade and this result in frequent robberies on highways and even within cities. Although there are various researches done on the card payment industry in general, there is no meaningful research done in the airline industry that investigates why card frauds are unproportionately high in the industry and on why card payment system in Ethiopia is lagging behind.

Unlike many other organizations whose operations are limited only to the home country, Ethiopian Airlines operates in five continents, eighty five international destinations and connecting Africa to the rest of the world (Ethiopian Airlines, 2015). Operating globally means it is not an option for the airline to go out of the traditional payment methods and offer convenient distribution channels and payment methods to its customers. Failure to do so gives competitors the cutting edge and enable to snatch customers out of hand. Studies by Atmosphere Research Group (2012) show that seven out of ten travelers have no sense of brand loyalty, that means customers need convenience among many other things. Moreover, the world is fastly moving to the cashless environment and the airline needs to follow that move.

On the otherhand, the writer hypothesizes that management and employees of the airline seems to have limited knowledge and lack awareness of the card payment industry's rules and regulations governing such payment methods; the pervasiveness of credit card fraud and how it affects merchants; how fraudsters are using credit cards to steal billions of dollars each year and how to control and manage this growing type of fraud.

In the writer's opinion, therefore, this knowledge gap may be one of the reasons that expose the airline to higher chargeback or revenue losses. This is the reason that motivates the researcher to work in this area. The researcher believes that this paper is meant to build more awareness to the airline staff about this growing problem and to offer insights which aid the airline from becoming victim of credit card fraud and to use the card payment method effectively and increase its revenue by developing a holistic payment strategy.

1.3. Research Questions

The researcher believes that this paper answers the following specific questions related to the effectiveness of Ethiopian Airlines credit card sales management system.

- Do Ethiopian Airlines management and employees have awareness of the rules and regulations of a card payment industry?
- Does the airline provide adequate recurrent training to operational and back office staff on credit card acceptance and fraud management?
- Does Ethiopian Airlines have strong internal control governing its card acceptance procedures and handling chargeback and fraud analysis?
- Are chargeback or fraud rates increasing over time at Ethiopian Airlines and causing the airline to lose more revenue?
- Does Ethiopian Airlines have well-organized and structured credit card desk equipped with adequate staff and well integrated information systems?

1.4. Objectives of the study

1.4.1. General objective

The overall objective of the thesis is to assess credit card sales management system of the Ethiopian Airlines with a view to propose critical success factors.

1.4.2. Specific objectives

In order to achieve the overall objective stated above, the study accomplished the following specific objectives:

- Assess whether travel agents and sales officers of Ethiopian Airlines strictly follow best practices and the guidelines set by the PCI in processing credit card sales transaction and chargeback or fraud handling.
- Assess whether these agents and officers take sufficient recurrent training to enable them to have knowledge about how to effectively process credit card sales transactions and how to manage chargeback or frauds.

- Assess whether the airline has strong internal control systems and fraud management tools and strategies to prevent, detect, and make corrections timely;
- Assess whether the airline has adequately staffed credit card desk with skilled experts working on credit card sales management, credit card risk analysis and
- Assess whether the airline has automated and seamless information systems that enable the airline get real time data on its credit card sales, collections from payment consolidators and chargebacks or card frauds.

1.5. Significance of the study

This study has investigated current practices of the airline's credit card sales management system and identified the factors that would reduce the associated risk and contribute to business success. Through identification of critical success factors for effectively dealing with risks associated to credit card sales, the study made important contribution both to research and practice.

More specifically, the researcher believes that the result of this research project has the following significances:

- This research paper could be used as an eye opener for those who are interested to conduct a more detailed and comprehensive study regarding the Airline industry in general and at Ethiopian Airlines in particular.
- Moreover, it provides constructive feedback about the effectiveness of Ethiopian Airlines internal control and on the current practices over card acceptance and card fraud management strategies.
- Finally, the results of the study can prove to be of great importance to fill the gap in the knowledge or to gain a clearer insight onto how to accept credit cards, handle chargebacks and manage card frauds.

1.6. Scope of the study

The scope of the study was confined to surveying, interviewing and documentary analysis of the purposely sampled officials of the airline; agents; and acquiring bank staff in order to identify the factors relevant for the effectiveness of the airlines' credit card sales management system. As such, debit cards and alternative payment methods such as mobile payments, PayPal and others available in the market as a sales distribution channel today were not part of this study.

1.7. Limitations of the study

Due to time constraint and limited data access relating to the experiences of other airlines, especially those who are major competitors to Ethiopian Airlines, the researcher did not include fraud losses and fraud rates of other carriers. Moreover, this study was made with a mixed research approach using data almost only for one airline, Ethiopian Airlines, except that some data about the card payment and the airline industry were taken. The researcher therefore, suggests that future study shall be undertaken with data from other airlines to make important comparisons between airlines and to see why the fraud rates are exceptionally high with the airline industry.

1.8. Organization of the paper

The paper is divided into five chapters. Chapter one is the introduction part which contains background of the study, statement of the problem, the purpose of the research, research questions, scope and limitation of the study, and organization of the research paper. Chapter two provides the review of related literature such as the parties involved and the major processes of Credit Card transactions, chargeback handling, and fraud management. Chapter three discussed the methodology followed in this study. Chapter four presents the current practices and challenges of handling credit card sales in Ethiopian Airlines. Finally, chapter five discusses the major findings of the study and outlines important propositions for future research and relevant recommendations to effectively deal with risks associated to credit card sales.

Chapter Two: Review of Related Literature

2.1. Introduction

Many changes in the business environment in recent years have caused changes to the way organizations do their businesses. The increasing competitiveness of the global business environment means that firms increasingly need to search for new ways of doing business and to adopt emerging technologies (Earnst & Young, 2011). From payment processing perspective alone the emergence and growth of the various alternative payment methods is a remarkable change today. To remain competitive in the face of this increased global competition, firms around the world are adopting new service technologies.

The exchange of goods and services has always been a central part of society. Coins and bills support this exchange and go back as far as 3000B.C. in Mesopotamia. However, it is not always convenient to carry money around to pay for what you need, especially for larger value purchases or when travelling. If you can't pay immediately though, how do you get a potential merchant to trust you and hand over the items or services, you want and in return for a promise to be paid later? It was this need, the ability to have access to your funds at a distance, which drove the development of the payment systems that we have today (Helldorff, 2014).

The origins of the credit card do not stretch back too far. According to a history written by Ben Woolsey and Emily Starbuck Garson for credit-cards.com, the modern version of the card made its debut about sixty five years ago. The "Universal Air Travel Plan" or UATP led the development in the business travel industry. Founded in 1936, the Air Travel Card, as it was known initially, was an early innovator and pioneer of the charge card industry, developing such industry standards as the magnetic stripe and lodged accounts. Its main purpose is to streamline the billing between airlines and their customers, offering the lowest administrative costs of any travel payment product (UATP, 2011). UATP were then the

first cards in the world and these were yet another predecessor of today's credit cards. The first bank-issued card was introduced in 1946 by a New York banker.

1950 was a turning point for credit card business and when the concept of customers paying different merchants using credit card was expanded. It was Ralph Schneider and Frank McNamara who invented and became the founders of Diners Club Card. Although originally intended to pay for dinners only (hence the name of the card), cardholders were soon able to make purchases at a wide range of travel and entertainment related merchants, making it the first "Universal Card". Diners Club had no real competition until 1959, when American Express entered the market with a similar charge card. All of these cards were charge cards, where the purchases were made on credit, but the full bill had to be paid at the end of the month (Helldorff, 2014).

In Europe, the card business developed quite differently to that in the U.S. Cheques dominated the cash-less payments market there. The adoption of credit cards in Europe was much slower than in the U.S. or Canada. In some countries, acceptance still remains low as the use of a credit card system depends on the banking system of each country. Japan remains a very cash oriented society, with credit card adoption being limited mainly toward the largest of merchants (Helldorff, 2014). While the plastic card has been the standard for a half century, recent developments show alternative forms of payment rising to prominence, from online services such as PayPal to credit card key fobs to chips that can be implanted into cell phones or other devices (CreditCards.com, 2015).

2.2. Airline distribution and factors affecting distribution strategy

Airlines have been collecting payment for tickets since commercial flying began and have been innovators in the online world (Helldorf, 2014). In the 50 years since the airline industry began to teach the rest of the world how to conduct business electronically, much has been changed within and across airline distribution. Traditionally, travel agents processed distribution activities or payments on behalf of the airlines and the funds arrived

at the airlines' accounts almost automatically through various systems like the IATA Billing and Settlement Plan (Helldorf, 2014).

Airlines want to enter new markets and reach new, emerging customer segments and they need to be familiar with local payment behaviors and the payment methods relevant to that market (Helldorf, 2014). Airlines utilize a broad number of distribution channels and processes to bill credit transactions. The possible airline distribution channels include direct sales through own sales offices, call centres, websites and indirect sales by means of traditional travel agents, and tour operators. Each of the major distribution channels are briefly described below.

- **Direct Sales:** Direct sales are handled by the airline itself. Sales methods may include Mail Order or Telephone Order (MOTO), Web-site or E-Commerce, Sales Offices owned by the Airline at the Airport Ticket Office ("ATO") or City Ticket Office ("CTO").
- **Travel Agencies:** Most airline tickets are sold through travel agents.
- **General Sales Agents (GSAs)** are third party vendors contracted to sell services by the airline, generally substituting as the airline's sales office in countries of low volume.

Accessibility, efficiency and cost are the major factors affecting the choice of airline distribution channels. To reduce costs associated with distribution through travel agents and Global Distribution Systems (GDS), airlines were keen to increase the proportion of direct distribution – through call centres, the internet and more recently through mobiles, and social media (Mason, 2008).

2.3. Payment methods used in the airline industry

Since long time (3000B.C. in Mesopotamia), cash, cheques, and credit cards were the predominant payment methods used in the airline industry (Helldorff, 2014). Currently, international credit cards, debit cards, direct debit and bank transfers, electronic wallets (e-wallets), prepaid cards, mobile payments and vouchers and gift cards are also used as payment method in the industry. Cash is still very important in countries with limited banking infrastructure and low payment card penetration. However, international credit cards are a corner stone of payments in the air transport industry. They account for a very large proportion of the airline payment transactions. Credit cards are fully embedded in all airline systems and processes, giving them an advantage over all other alternative payment options (Helldorff, 2014).

Payment methods in the airline industry are standardised by IATA rules and according to Helldorff (2014) every payment system has to fulfil three requirements: it has to identify the buyer to the seller and the seller to the buyer; it has to be a guarantor to both the seller and the merchant; and finally it has to be the initiator of a payment transaction.

2.4. Selecting appropriate payment method(s)

Under section 2.2 and 2.3 above, the writer discussed the basics of airline distribution channels and the common payment methods used in the airline industry; it is therefore time to turn attention to the common criteria used to select appropriate payment method(s) with optimal balance. The processing of payments is a crucial element to the sales process. There are various issues to be considered when processing payments – what channels to support, what banks and financial institutions to deal with, what payment methods to support, how to manage currencies, fraud, reconciliation etc.

Customers' convenience should always be at the heart of the decision in the selection of payment methods (Lyon, 2008). In order to reach new customers and increase sales, businesses must offer their customers the opportunity to pay in the way most convenient for

them. The risks, costs and implications of these payment methods may be significant and in some cases tie up much needed capital. On top of this there are more partners to deal with, more players and service companies emerging on the market place, compliance issues, reporting and reconciliation requirements, all in a multi-currency environment where service and reliability are crucial (Lyon, 2008).

For businesses selling their products or services online with multiple currencies at multiple locations, the acceptance of global scheme cards is central to the payments strategy. The online payments business has been dominated by the global credit card schemes – Visa and MasterCard. While current trends suggest that there will be more players and more payment methods in the online market space, the importance of the global card schemes will remain. Risk, cost and compliance to rules and regulations shall therefore be the key considerations here (Lyon, 2008).

Within many country borders, domestic payment systems remain and often dominate offline and online sales in those regions and/or countries. Hence, accepting the local payment method may become a mandatory need if one is to sell in that region. However accepting “local payment methods” can add a layer of complexity that can make their processing in the first place a poor decision. They can give rise to additional local banking arrangements, different fraud requirements and reconciliation all of which should be taken into account (Lyon, 2008).

Finally it is important to make a cost-benefit analysis by determining the development and operational costs and comparing this to the increased sales.

2.5. Credit Card Transaction Processing Flows

In today’s information and communication technologies credit card payments have become simultaneously easier and more complex (Visa, 2008). Electronic terminals and card acceptance devices make transaction processing automatic and seemingly effortless, raising

potential profitability. However, they also create increased possibilities for processing mistakes and fraudulent transactions that can result in copy requests and chargebacks. In addition, the walls between card-present and card-absent transactions have become less obvious as growing numbers of traditional “brick and mortar” merchants launch e-commerce websites, transforming themselves into “click and mortar” businesses. Such merchants must, in effect, be “bilingual”- familiar with both card-present and card-absent procedures (Visa, 2008).

The processes for accepting credit cards vary according to the situation. When accepting credit cards it is strongly recommended that the travel agent or the ticket agent shall confirm that the card is valid and active, that the cardholder identity can be authenticated, and that the transaction is legitimate (Visa, 2008). In an attempt to remain competitive, and in a market where customers expect to purchase travel from the comfort of their home, travel agents often accept credit card payments from first-time customers with very little identifying information. By supporting this type of distribution, travel agents and airlines take the risk that customers are perpetrating fraud, so the need to weigh the pros and cons.

2.5.1. Who does what to make a payment happen?

Typically, a credit card payment transaction involves interaction among various stakeholders including cardholders, merchants, acquirers, card scheme, card issuers, payment service providers, and payment networks. Each of these stakeholders has an incentive to play its specific role in completing the payment transaction (Helldorff, 2014). The below section of the paper provides a brief overview of the major participants in the payment process.

- **Cardholder** – is a customer of the merchant and the issuing bank that wants to buy goods and services through credit card.
- **Merchant** – is the contractual party selling the goods or service, an airline in this case that transacts with the cardholder with credit card. A merchant accepts payment from

the cardholder by swiping the user's card at its terminal, increasing the chance of a sale by accepting popular cards used by cardholders. Merchant contracts with an acquirer or a member bank to accept card payments for goods or services provided. The merchant is expected to pay commission to the acquiring bank per the service agreement that the two parties concluded.

- **Acquiring bank or merchant bank** - The acquiring bank is the financial institution licensed by a credit card organization to help a merchant to fulfil its obligation to accept credit cards and that maintains a contractual relationship with the merchant separately. As a license holder the bank guarantees to take on the responsibilities and risks associated with acquiring a merchant. Acting as a "middle man," the acquiring bank collects all payment transactions the merchant has performed during a day and submits them to the respective card schemes for settlement. Once they are processed, it accepts the deposits from the card schemes and forwards them to the merchant's accounts (Helldorff, 2014).
- **Card scheme / credit card association/ credit card organization** - Card schemes, such as Visa, MasterCard, American Express, Diners Club etc. act as the link between the issuer bank and the acquiring bank. The card scheme ties all the participants together. The associations do not directly issue credit cards. Their main responsibility is to develop and enforce the rules and regulations governing how transactions, services, and disputes are to be handled and to manage the routing of transactions between their participants. The rules are designed to eliminate fraud, promote use of credit cards in financial transactions, and to accommodate the various industries that desire to accept credit cards as payment for goods and services (IATA, 2010).
- **Issuing bank or cardholder's bank**- is any card association member financial institution, bank, credit union, or company that issues, or causes to be issued, credit cards to cardholders (Helldorff, 2014). It authorises or declines transactions the

cardholder wants to perform with the card(s) and bills the cardholder for all purchases made using the card(s). The issuing bank transfers funds to acquiring banks to cover purchases made by the cardholder, and receives the cardholder's payment at the end of the billing period.

2.5.2. Key Functions

Completing a payment requires that multiple sub-transactions go back and forth between the various payment entities described above. These include the authorization request, the confirmation, transaction submission, the clearing and settlement processes and the fund transfer to the merchant. Each major functions of the credit card transaction has various activities within it and in the below section of this paper we try to see the major activities in brief.

a) Transaction Authorization

An authorization request is a request to the cardholder's issuing bank to authorise a payment transaction that the cardholder would like to perform in return for the goods or services that they are purchasing from the merchant (Helldorff, 2014). Authorizing transactions is a critical function of acquirers and issuing banks don't take this promise lightly. Upon receiving an authorization request, the issuing bank would follow a number of checks to ensure that the transaction is genuine (that the cardholder is the real cardholder) and that the cardholder has sufficient funds to cover the transaction.

Operationally, when the card is swiped at the merchant's POS terminal, the acquirer receives an authorization request from the terminal. This request contains transaction details such as the cardholder's information and amount of the transaction. The request is forwarded to the card association/network, for example Visa /MasterCard, which in turn validates the availability of funds with the issuing bank. The issuing bank sets aside the funds from the cardholder's account for the transaction and sends an authorization code to the network. The network forwards the code to acquirer and then to the merchant's POS

terminal. At this point, the funds are not yet transferred to the merchant's account but the issuing bank agrees for a future settlement with the acquiring bank and, in turn, the merchant. After the authorization is completed, the merchant records the sales transaction information and sends or submits it to the acquirer for processing at the end of the day.

During the authorization process, the merchant's sales agents should receive one of the following responses (or one that is similarly worded) from the issuing bank.

- **Approved:** This means the card issuer approves the transaction. This is the most common response from the issuing bank. It is generally recognized that receipt of an approval code from the issuing bank does not guarantee the transaction and that any such approval code or other authorization does not (and shall not be deemed to) guarantee that the charge will go undisputed (IATA, 2011).
- **Declined or card not accepted:** Card issuer does not approve the transaction. The transaction should not be completed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account. This may be due to various reasons including invalidity of the card, card may be reported as lost or cardholder may not have sufficient balance to support the transaction.
- **Need for further information:** Card issuer needs more information before approving the sale. The merchant should call its authorization centre and follow whatever instructions are given.

When a transaction is approved (as in the first case above), the point-of-sale terminal automatically prints a sales receipt. When a negative or alert message is received, the response is displayed on the point-of-sale terminal, and no sales receipt is printed. Whatever the message, you should continue to treat the customer courteously so as not to arouse alarm or suspicion. .

Cardholder Verification and Identification: The final step in the card acceptance process for transactions requiring a signature is to ensure that the customer signs the sales receipt and to compare that signature with the signature on the back of the card. If possible, the selling agent should check the two signatures closely for any obvious inconsistencies in spelling or handwriting. While checking the signature, the agent should also compare the name and account number on the card to those on the transaction receipt. For magnetic-stripe card transactions, match the name and last four digits of the account number on the card to those printed on the receipt.

Although a card scheme's rules do not preclude merchants from asking for cardholder ID or passport except in the specific circumstances, merchants cannot make an ID or passport a condition of acceptance. Some card schemes like Visa believes merchants should not ask for ID as part of their regular card acceptance procedures. Laws in several countries also make it illegal for merchants to write a cardholder's personal information, such as an address or phone number, on a sales receipt.

The selling agent shall use common sense and appropriate caution when evaluating any customer behaviour or other irregular situation that may occur during a transaction. The merchant shall also keep cardholder's account numbers and personal information confidential. Cardholders expect you to safeguard any personal or financial information they may give you in the course of a transaction. Keeping that trust is essential to fraud reduction and good customer service. Cardholder account numbers and other personal information should be released only to your acquirer or processor, or as specifically required by law.

The below diagram represents the flow of the credit card transaction processes with the major parties involved in a credit card transaction.

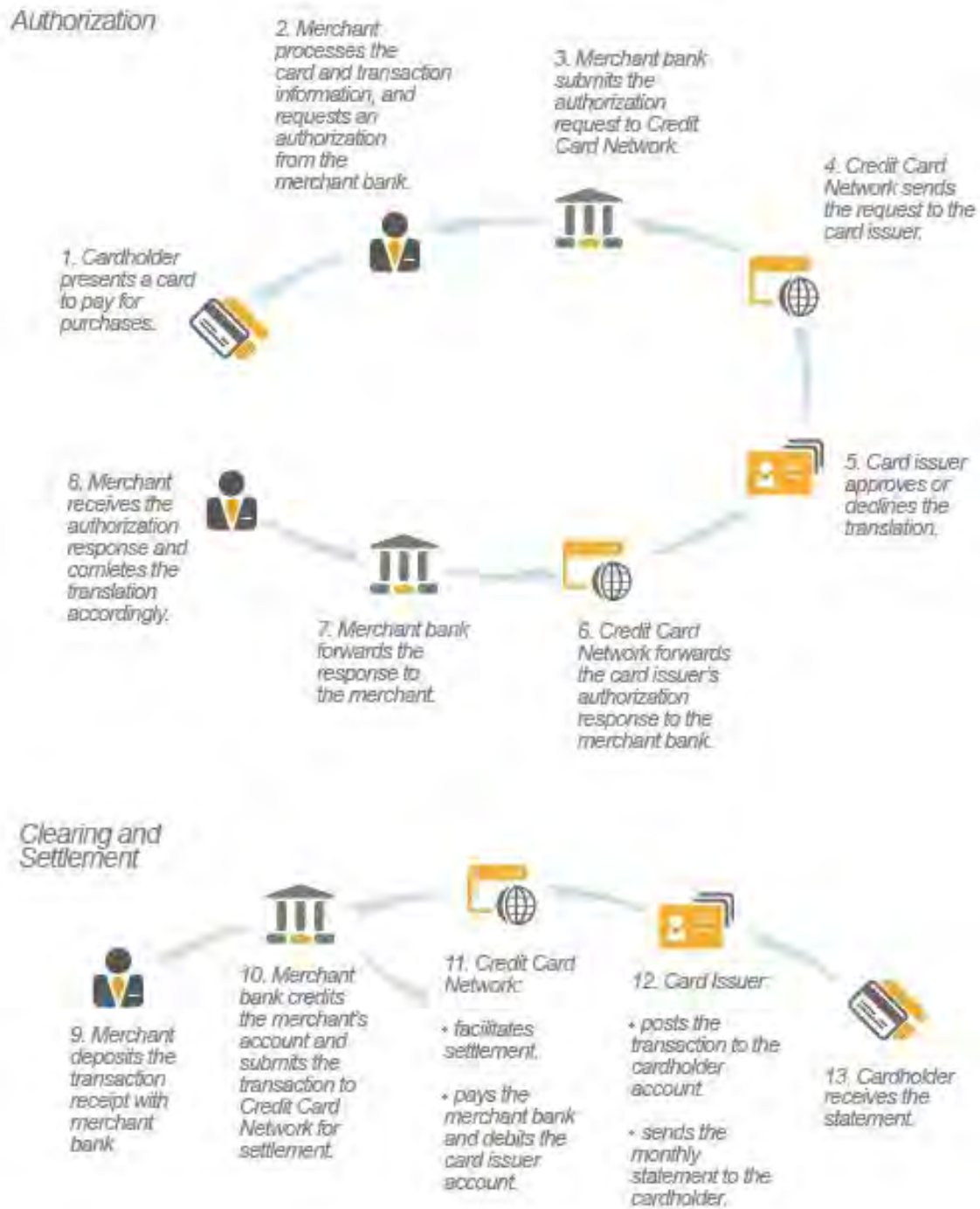


Figure 1: Diagrammatic description of credit card processing (Source: Visa Card Acceptance Guidelines, 2014)

b) Transaction Submission

Credit card payments are not completed until the transaction information along with the approval code received is submitted to the processing bank or the acquirer. Typically transactions are submitted electronically and all point-of-sale (POS) and virtual payment processing systems are programmed to automatically do that at pre-defined intervals, usually at the end of the business day. Transactions can be submitted any time immediately after the authorization up until several days.

c) Clearing and Settlement

Clearing is a process through which a card issuing bank exchanges transaction information with a processing bank and occurs simultaneously with the settlement. At the end of every day acquiring banks collect the transactions their merchants have performed during the day, sort them and forward to the respective clearing and settlement systems of each card schemes. The card schemes then forwards the transactions to the various card issuing banks.

Typically, merchant accounts are funded between 24 and 72 hours after the purchase transaction. But the time of crediting the merchants bank account depends on the agreement between the merchant and the acquiring bank as the latter usually holds back the amounts settled by the issuing bank to cover bad transactions. Such bad transactions include chargeback claims from cardholder that may come at a latter date or to protect itself from possible risks arising from un-flown tickets, should the airline that they acquire go out of business (Helldorff, 2014).

d) Reconciliation and analysis by the merchant

Once the merchant receives settlement report from the acquirer and bank statement from its bank and ensures that collections have been done, the merchant shall take reconciliation of

sales data and sales collections. Usually, there is a difference between the ticket value and the amount collected from the acquirer due to merchant fee, refunds, chargebacks, and exchange rate differences. The merchant shall, therefore, take timely reconciliation to account its revenue and take appropriate accounting action.

2.6. Types of credit card transactions

Sales using credit cards can be in card-present or card-not-present transactions and as indicated above the walls between these two transactions have become less obvious due to the application and effect of latest technologies. Proper card acceptance begins and ends with sales staff and is critical to customer satisfaction and profitability (Visa, 2014)

2.6.1. Card-present transactions

Card-present transactions are those in which both the card and cardholder are present at the point of sale. In traditional sales environments, merchants are required to take all reasonable steps to assure that the card, cardholder and transaction are legitimate. In a card present environment the merchant has the advantages of physical verification such as signature check, photo identification, etc. (Bhatla, 2003).

For face-to-face transactions the selling agent shall capture the card details (card number, cardholder name, expiry date, and where applicable, effective date of the card) by use of a card imprinter, or electronic card reader or card swipe (IATA, 2011). In a card-present transaction the signature of the cardholder on the validated approved credit card charge form (CCCF) shall be witnessed by the agent, and matched against the signature on the reverse side of the card.

2.6.2. Card- Not- Present Transactions (CNP)

CNP transactions happen in an environment where a transaction is completed in the absence of both the cardholder and the card. Transactions in this environment include mail order or telephone order (MOTO) and Internet transactions and the merchant has no chance

for physical verification. The card not present (CNP) transaction therefore, exposes the merchant for additional credit card risks and it is essential to understand these risks and take every possible preventive strategy by implementing effective security systems.

2.7. Credit Card Features and Security Elements

All cards branded with the major international card companies have security features for merchants to check during a transaction. The merchant and its agents are the first line of defence (MasterCard, 2008). Every credit card contains a set of unique design features and security elements developed by card scheme to help merchants verify a card's legitimacy. It is therefore, essential to train sales staff to take a few seconds to look at the card's basic features and security elements after they have swiped the card and are waiting for authorization. Checking card features and security elements helps to ensure that the card is valid and has not been altered in any way. Holding onto the card for sometimes during transaction allows the sales agent time to check card features and security elements and to compare the cardholder signature on the card with the signature on the supporting documents to the transaction (The University of California, 2014).

By knowing what to look for on a card, the merchant can avoid inadvertently accepting a counterfeit card or processing a fraudulent transaction. The following figure shows what to look for on a Visa card.



Figure 2: Checking card features and security elements (source: PCI-DSS: Card Present - Security Elements- 2014)

2.8. Chargeback and chargeback prevention

A chargeback is a transaction returned through interchange by an issuing bank to an acquiring bank and then to the merchant. A transaction may be returned because of rules and regulations violations, because the sale is disputed by a cardholder, or as a result of fraud. In the case of cardholder dispute, the merchant has the opportunity to appeal and prove that the sale is valid.

2.8.1. Why chargebacks occur

As consumers using a credit card, we have a guarantee that if we were not involved in a transaction that has been billed to our account, or we did not receive the product or service promised, we can question the charge and charge it back. Merchants and travel agents engage in a process that must be managed to respond to these inquiries, or chargebacks (Airlines Reporting Corporation , 2010). The diagram below represents the chargeback cycle showing the main steps.

The Chargeback Life Cycle

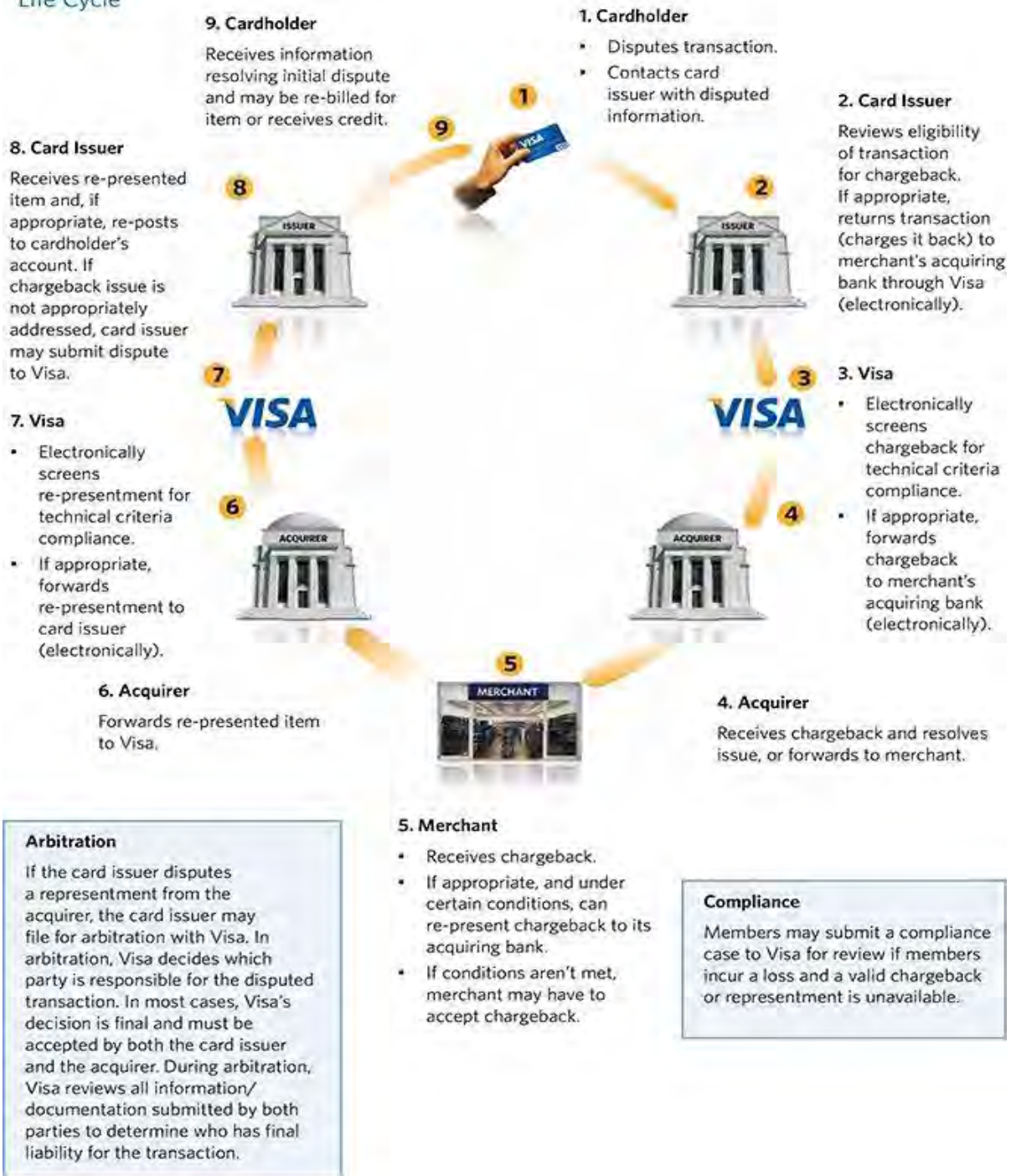


Figure 3: The Chargeback Cycle (Source: Card acceptance guidelines for merchants (Visa, 2008))

2.8.2. Responding to chargebacks

As soon as the merchant receives the chargeback from the acquirer, it passes same on to the travel agent for possible explanation and supporting documents. The travel agent should therefore take various actions to respond to inquiries or debit memos received from a carrier. The agent shall first of all contact the customer to explain the charge. In all cases, it is necessary to provide the most professional, legible, and detailed documentation available to back up the charge. It helps to provide details of what the transaction represents and what the customer received, copies of invoices provided to customer, signed acknowledgement of Terms and Conditions, signed and imprinted Universal Credit Card Charge Form (UCCCF). In addition, the agent shall include all relevant documents such as itineraries, invoices, copies of tickets, e-mails, etc. Some chargebacks can be resolved easily without the merchant having to lose the sale. The key here is to always supply as much information and supporting documents as soon as possible to your acquirer to help them remedy the chargeback.

A cardholder can dispute a charge any time within 180 days from the transaction date of the original sale or the date of discovery of the issue. However, in some instances the time frame may be longer or shorter depending on the specific reason code. A merchant can receive a chargeback when it received an approval code on the transaction from the issuing bank since an authorization code simply verifies that the card is in good standing, has not been reported lost or stolen at the time of the transaction, and has sufficient funds available for the amount of the transaction you are attempting to process. An authorization code does not guarantee that you will not receive a chargeback.

Although the merchant probably cannot avoid chargebacks completely, it can take steps to reduce or prevent them. Many chargebacks result from easily avoidable mistakes, so the more the merchant knows about proper transaction-procedures, the less likely it will be inadvertently do, or fail to do, something that might result in a chargeback. Of course chargebacks are not always the result of something merchants did or didn't do. Errors are

also made by merchant banks, card issuers, and cardholders as indicated above that the merchant granted an authorization for an invalid card (Visa, 2008).

Timeliness is also important when attempting to remedy a chargeback. Each step in the chargeback cycle has a definite time limit during which action can be taken. If the merchant or merchant bank do not respond during the dispute period specified on the request, which may vary depending on the service agreement between the two (merchant and merchant bank), the merchant will not be able to remedy the chargeback. Although many chargebacks are resolved without the merchant losing the sale, some cannot be remedied. In such cases, accepting the chargeback may save the time and expense of needlessly contesting it by the merchant (Visa, 2008).

2.8.3. How to minimize chargebacks

According to the card schemes' chargeback management guidelines for merchants, most chargebacks can be attributed to improper transaction processing procedures and can be prevented with appropriate training and attention to detail. Although the merchant can't avoid chargebacks completely, it can take steps to reduce or prevent them. Many chargebacks result from easily avoidable mistakes, so the more you know about proper transaction-processing procedures, the less likely the merchant will be to inadvertently do, or fail to do, something that might result in a chargeback. For card-present transactions the merchant's sales agents shall take the steps mentioned under the card authorization part above and follow best practices to minimize chargebacks.

The best practices available to minimize chargebacks in the case of card present transactions may not be applicable for card-not present transactions. The merchant therefore, needs to apply different mechanisms to minimize the possibilities of chargebacks in the case of CNP transactions and these mechanisms include Address Verification Service (AVS) and Card Verification Values (CVV2).

AVS is a risk management tool that enables a merchant to verify the billing address of a customer presenting a credit card for payment (Helldorff, 2014). The merchant includes an AVS request with the transaction authorization and receives a result code indicating whether the address given by the cardholder matches the address in the issuer's file. The issuing bank compares the address information in the authorization request message with its database of information about the cardholder. A "Partial" or "No Match" may indicate fraud risk.

If a merchant believes that it has AVS, AVV2, or any other compelling information representment rights on a chargeback transaction, the merchant can work with its acquirer to ensure that all supporting evidence for the representment is submitted to the issuing bank or the card association. In the card-not present sales environment, CVV2 is an excellent tool for verifying that the customer has a legitimate card in hand at the time of the sales order (Visa, 2011).

Another mechanism for merchants accepting card not present transactions with Visa branded cardholders is to use Verified Visa Chargeback protection. Visa's security strategy is built on the belief that the most effective way to address the multiple types of fraud is to employ multiple layers of security and fraud protection (Visa, 2011). Based on the 3-D Secure protocol, the VbV service verifies the authenticity of cardholders to participating merchants. It allows cardholders to choose a password through their card issuer, and use it to authenticate themselves while making a purchase. This helps ensure that their card number cannot be fraudulently used at an Internet merchant web site (Visa, 2011).

According to the Global Visa card-not-present merchant guide 2011, merchants offering VbV to their customers must incorporate a software module called a Merchant Plug-In (MPI), as part of their e-commerce server application. Merchants who opt to implement VbV should use PCI compliant vendors and payment solutions. Verified by Visa provides merchants with cardholder authentication on e-commerce transactions. This mechanism

helps reduce e-commerce fraud by ensuring that the transaction is being initiated by the rightful owner of the Visa account. This gives merchants greater protection on e-commerce transactions. Another advantage of using VbV mechanism is that participating merchants are protected by their acquirer from receiving certain fraud-related chargebacks, provided that transaction is processed correctly.

In general, for CNP transaction, a manually keyed-in authorization request should also include the security code:

- 3 digits known as CVC2 for cards at the back of MasterCard cards
- 3 digits known as CVV2 for cards at the back of Visa cards
- 4 digits known as CID for cards at the back of American Express cards.
- 3 digits known as CVV2 for cards at the back of Diners Club cards
- 3 digits known as CVV for cards at the back of Discover cards

For the sake of simplicity, such security codes will be referred to in this paper under the generic term “CVX2”. The CVX2 is unique to each card and helps the card issuer to spot fraudulent usage of the card: when the cardholder cannot provide the genuine information it is likely that misuse of the card is taking place. Merchants must insist that the customer provides the CVX2 for CNP transactions. Due to rigorous card industry manufacturing standards this information is highly resistant to normal wear and tear so it is unlikely that a legitimate cardholder would not be able to provide the CVX2.

2.9. The Fraud Management Strategies

With fraud continually surfacing in new and unexpected ways, a financial institution's profitability, reputation and customer satisfaction are always on the line (MasterCard, 2011). Furthermore, today's sophisticated fraudsters are attacking from many angles, across channels and with alarming success. Managing the cost of fraud extends well beyond the overt financial losses. Reputation loss, as measured by increased customer attrition and difficulty winning new customers, contributes to the total costs of managing fraud just as surely as the investments you make in anti-fraud technology. .

Credit card fraud has been a world-wide problem for years and become a healthy and growing means of stealing billions of dollars from credit card companies, merchants and consumers (Sheridon, 2008). However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of modus operandi to commit fraud (Bhatla, 2003).

Contrary to popular belief, merchants are far more at risk from credit card fraud than the cardholders. While cardholder may face trouble trying to get a fraudulent charge reversed, merchants lose the cost of the product sold, pay chargeback fees, and fear from the risk of having their merchant account closed (Bhatla, 2003). The internet is becoming extremely attractive to fraud perpetrators. However, recent technical developments are showing some promise to check fraud in the card not present scenario.

2.9.1. Common Fraud Schemes or techniques

While lost or stolen card is the most common type of fraud, others include identity theft, skimming, counterfeit card, mail intercept fraud and others. The following table summarises the modus operandi for credit card frauds and their percentage of occurrence. The table shows that stolen and counterfeit cards together contribute to more than 60% of fraud losses according to figures published by both MasterCard and Visa.

Method Percentage	Percentage of Fraud
Lost or stolen card	48
Identity theft	15
Skimming (or cloning)	14
Counterfeit card	12
Mail intercept fraud	6
Other	5

Table 1: Methods of Credit Card Fraud and their percentage of occurrence (*Source: Celent Communications, January 2003*)

As indicated above, there are many ways in which fraudsters execute a credit card fraud. As technology changes, so do the technology of fraudsters, and thus the way in which they go about carrying out fraudulent activities. Generally, frauds can be broadly classified into three categories, such as traditional card related frauds, merchant related frauds and internet frauds. In the below sections of this paper we try to see the different types of methods for committing credit card frauds in brief.

i. Card related frauds

- **Application Fraud:** This type of fraud occurs when a person falsifies an application to acquire a credit card. Application fraud can be committed either by assuming identity, where an individual illegally obtains personal information of another individual and opens accounts in his or her name, using partially legitimate information or by means of financial fraud.
- **Lost or stolen credit cards:** A card is lost/stolen when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. When a credit card is lost or stolen the criminal gains direct access to the individual's credit

card account. The criminal may also gain access to other personal information about the individual as the lost and stolen credit cards are often contained in wallets, purses and briefcases (Stanley, 2002). This type of fraud is in essence the easiest way for a fraudster to get hold of other individual's credit cards without investment in technology. It is also perhaps the most common form of abuse in the industry and the hardest form of traditional credit card fraud to tackle (Bhatla, 2003).

- **Account takeover:** This type of fraud occurs when a fraudster illegally obtains a valid customers' personal information. The fraudster takes control of (takeover) a legitimate account by either providing the customer's account number or the card number. The fraudster then contacts the card issuer, masquerading as the genuine cardholder, to ask that mail be redirected to a new address. The fraudster reports card lost and asks for a replacement to be sent.
- **Fake and counterfeit cards:** the creation of counterfeit cards, together with lost or stolen cards poses the highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. The common techniques used for creating false and counterfeit cards include erasing the magnetic strip, creating a fake card, altering card details and skimming (Bhatla, 2003). As the fastest growing type of credit card fraud, this scheme makes up 37 percent of funds lost through credit card fraud (Sheridon, 2008). This type of fraud occurs when the criminal steals legitimate credit card information, through skimming or other methods, and makes a fake card. The production of counterfeit cards has become easier with advances in technology. The processes used to produce the card, along with the production of holograms, have allowed counterfeit cards to look more accurate and legitimate (Sheridon, 2008).

Most cases of counterfeit fraud involve skimming, a process where genuine data on a card's magnetic stripe is electronically copied onto another. Skimming is the unauthorized capture

and transfer of payment data to another source, for fraudulent purposes (PCI SSC, 2009). Skimming takes place unknown to the cardholder and is thus very difficult, if not impossible to trace. In other cases, the details obtained by skimming are used to carry out fraudulent card-not-present transactions by fraudsters. Often, the cardholder is unaware of the fraud until receipt of a statement showing purchases they did not make. A merchant has the additional challenge and cost of dealing with a skimming event to include the cost of forensics and system analysis, system upgrades based on recommendations, industry fines, lawsuits, employee terminations, loss of goodwill, and other liability concerns (PCI SSC, 2009).

ii. Merchant related frauds

Merchant related frauds are initiated either by owners of the merchant or their employees. The types of frauds initiated by merchants include merchant collusion and triangulation. Triangulation is when a merchant offers a product at a very cheap price through a web-site. When a customer seeks to buy the product the merchant tells to customer to pay via email once the item is delivered. The merchant uses a fraudulent card number to purchase the product from a Web site and sends the product to the consumer, who then sends the merchant his or her credit card details via email. The merchant goes on operating in this way using the credit card numbers that have been sent from the consumers to purchase products, appearing for a short time to be a legitimate merchant before he or she closes the Web site and starts a new one (Sylvester, 2002).

iii. Internet related frauds

The Internet has provided an ideal ground for fraudsters to commit credit card fraud in an easy manner. Fraudsters have recently begun to operate on a truly transnational level. The most commonly used techniques in internet fraud are site cloning, merchant sites and credit card generators (Bhatla, 2003).

Site cloning is where fraudsters clone an entire site or just the pages from which you place your order. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services because the pages that they are viewing are identical to those of the real site. The cloned or spoofed site will receive these details and send the customer a receipt of the transaction via email just as the real company would. The consumer suspects nothing, whilst the fraudsters have all the details they need to commit credit card fraud (Sylvester, 2002).

2.9.2. Impact of Credit card frauds

Unfortunately, occurrences of credit card frauds have only shown an upward trend so far and the fraudulent activity on a card affects everybody, i.e., the cardholder, the merchant, the acquirer as well as the issuer (Bhatla, 2003). The focus of this paper is not to analyse the impact that credit card frauds have on all the players involved in transacting business through credit cards; rather it is to see the impact on the merchant alone.

Merchants are the most affected party in a credit card fraud, particularly more in the card-not-present transactions, as they have to accept full liability for losses due to fraud (Bhatla, 2003). In case, the merchant does not have any physical evidence (e.g. delivery signature) available to challenge the cardholder's dispute, it is almost impossible to reverse the chargeback. Therefore, the merchant will have to completely absorb the cost of the fraudulent transaction. In fact, this cost consists of several components, which could add up to a significant amount. The cost of a fraudulent transaction consists of costs of goods or services sold, shipping cost, card association fees, acquirer fee, administrative cost and loss of reputation (Bhatla, 2003).

2.9.3. Fraud prevention and management

With all the negative impacts of fraudulent credit card activities, financial and product losses, fines, loss of reputation, etc., and technological advancements in perpetrating fraud it's easy for merchants to feel victimized and helpless (Bhatla, 2003). However, technological advancements in preventing fraud have also started showing some promise to combat fraud.

Merchants, acquirers and issuers are creating innovative solutions to bring down on fraudulent transactions and lower merchant chargeback rates. One of the main challenges with fraud prevention is the long time lag between the time a fraudulent transaction occurs and the time when it gets detected, i.e., the cardholder initiates a chargeback. Analysis shows that the average lag between the transaction date and the chargeback notification could be as high as 72 days (Bhatla, 2003). This means that, if no fraud prevention is in place, one or more fraudsters could easily generate significant damage to a business before the affected stakeholders even realize the problem.

The various fraud prevention techniques are discussed below:

- a. Manual Review:** This method consists of reviewing every transaction manually for signs of fraudulent activity and involves exceedingly high level of human intervention. This can prove to be very expensive, as well as time consuming. Moreover, manual review is unable to detect some of the more prevalent patterns of fraud, such as use of a single credit card multiple times on multiple locations (physical or web sites) in a short span (Bhatla, 2003).
- b. Address verification system:** This technique is most applicable in a card-not-present scenario. Address Verification System (AVS) matches the first few digits of the street address and the ZIP code information given for delivering/billing the purchase to the corresponding information on record with the card issuers (Bhatla, 2003).
- c. The card verification method:** as discussed in the previous sections of this paper a CVM consists of a 3-or 4-digit numeric code printed on the card but is not embossed on the card and is not available in the magnetic stripe (Bhatla, 2003). The merchant can request the card holder to provide this numeric code in case of card-not- present transaction and submit it with authorization.

- d. **Negative and positive lists:** A negative list is a database used to identify high-risk transactions based on specific data fields. An example of a negative list would be a file containing all the card numbers that have produced chargebacks in the past, used to avoid further fraud from repeat offenders. Similarly a merchant can build negative lists based on billing names, street addresses, emails and internet protocols (IPs) that have resulted in fraud or attempted fraud, effectively blocking any further attempts. A merchant could create and maintain a list of high-risk countries and decide to review or restrict orders originating from those countries (ClearCommerce Corporation, 2001).
- e. **Payer authentication:** is an emerging technology that promises to bring in a new level of security to business-to-consumer internet commerce. The program is based on a Personal Identification Number (PIN) associated with the card, similar to those used with ATM cards, and a secure direct authentication channel between the consumer and the issuing bank. The PIN is issued by the issuing bank when the cardholder enrolls the card with the program and will be used exclusively to authorize online transactions.

When registered cardholders check out at a participating merchant's site, they will be prompted by their issuing bank to provide their password. Once the password is verified, the merchant may complete the transaction and send the verification information onto their acquirer (Bhatla, 2003).

Generally, a two-step fraud detection system such as an automated evaluation followed by a manual investigation process is highly recommended and becoming the best proactive for merchants to mitigate credit card fraud (Visa, 2011). The first step, automated order screening, should leverage your own data, third-party fraud prevention tools (such as IP Geo-location, device finger printing, fraud-scoring models, velocity checks, and more), as well as a variety of services made available by card schemes. These include Verified by Visa (VbV), Card Verification Value 2 (CVV2), and Address Verification Service (Visa, 2011).

The second step, orders that do not pass the first step should then be sent to your order review team for further scrutiny. Thus, it's critical that they are armed with the verification tools necessary to validate questionable orders, as well as a case management system to keep track of the orders in queue. The verification tools and the case management system enable the reviewers to process more orders in an effective and efficient manner (Visa, 2011).

Another important and latest development tool to mitigate credit card frauds is to use 3-D Secure Cards. 3-D Secure is an XML-based protocol designed to be an additional security layer for online credit and debit card transactions. It was developed by Visa with the intention of improving the security of Internet payments and is offered to customers under the name Verified by Visa. Services based on the protocol have also been adopted by other card schemes later on. This authentication is based on a three-domain model (hence the 3-D in the name). The three domains are:

- Acquirer Domain (the merchant and the bank to which money is being paid).
- Issuer Domain (the bank which issued the card being used).
- Interoperability Domain (the infrastructure provided by the card scheme, credit, debit, prepaid or other type of finance card, to support the 3-D Secure protocol). Interoperability Domain includes the Internet, MPI, ACS and other software provider

The main advantage for merchants using 3-D Secure cards is the reduction of "unauthorized transaction" chargebacks. One disadvantage for merchants is that they have to purchase MPI to connect to the Visa or MasterCard Directory Server. This is expensive (one time setup fee, monthly fee and per-transaction fee). Perhaps the biggest disadvantage for merchants is that many users view the additional authentication step as a nuisance or obstacle, which results in a substantial increase in transaction abandonment and lost revenue (Wikipedia).

2.10. Internal Control Framework

An internal control system is the process implemented to provide reasonable assurance that the company will achieve its objective(s). This reasonable assurance is obtained by means of safeguarding assets, maintaining sufficient records, providing accurate and reliable information, promoting operational efficiency, and adhering to prescribed managerial policies and procedures (Romney, 2012).

Developing an internal control system requires a thorough understanding of information technology (IT) capabilities and risks, as well as how to use IT to achieve an organization's control objectives. It is also helpful to understand the basic steps criminals use to attack an organization's information system. A well developed and well integrated internal control system performs three important functions: preventive, detective and corrective controls and it is a combination of these that provide reasonable assurance.

Companies using credit cards as a payment method must implement strong internal controls and safeguards to provide reasonable assurance that all credit card transactions are properly authorized, timely settled, and accurately and completely recorded; protect the security, confidentiality and integrity of cardholder information; and comply with several layers of laws, rules, standards and compliance regulations. The merchant's internal control systems shall also support the end-to-end payment processes.

Merchants have a responsibility to understand the unique issues of operating their e-commerce programs and to create internal policies and procedures to address those issues. Accepting a promise to be paid at some time in the future in return for goods and services that a merchant hands over to a customer is always going to be a bit more risky than getting the cash in your hands immediately (Helldorff, 2014). The merchant is the entry point of a transaction and they take on the role of "gate keeper" and must ensure that only "good" transactions get into the system. Good transactions are those that are carried out by genuine cardholders with genuine payment cards. The biggest part of the risk is therefore, carried by

the merchant (Helldorff, 2014). In the below sections of this paper the writer discussed an overview of the internal control system of a merchant pertaining to handling credit card payments.

2.10.1. Board and Management Supervision

The core of any business is its people –their individual attributes, including integrity, ethical values, competence and the environment in which they operate. They are the engines that drive the organization and the foundation on which everything rests (Romney, 2012). The more responsible management’s philosophy and operating style, and the more clearly they are communicated, the more likely employees will behave responsibly. If management has little concern for internal controls and risk management, then employees are less diligent in achieving control objectives. Management should therefore assess potential risks and rewards of using credit card as a payment method and clearly communicate same to all that are involved in the credit card handling activities, starting from transaction authorization up to fraud analysis and management.

The fact that the biggest part of the risk in accepting card payments is carried by the merchant means that the board and management supervision shall be strong and must ensure that the merchant has established a comprehensive risk management process for managing and monitoring the risks associated with its credit card activities. The Board and senior management of a merchant should receive and review regular reports which detail risk management information on its credit card operations such as the volume of credit sales through credit cards as compared to the total sales, trend reports, and chargeback and fraud rates (Helldorff, 2014).

Merchants therefore, need a holistic and effective strategy for their payment processing (Lyon, 2008). A holistic payment strategy in this case is a strategy that considers the core building blocks such as multiple sales channels, multiple currencies, local and global payment methods, chargebacks and frauds, revenue reporting and reconciliation, fraud management, compliance to the card payment industry’s rules and regulations, payment partners like

acquirers, the risks, costs and complexity of the payment processing etc., all need to be taken into account (Lyon, 2008).

Once developed the strategy should help to answer questions like: what policies and procedures to use, what payment methods are needed, what banking arrangements does the merchant need to support these, does the merchant need to use a Payment Services Provider, and how will the merchant manage fraud (Lyon, 2008).

2.10.2. Policies and procedures

It is management's responsibility to develop a secure and adequately controlled system (Romney, 2012). Management shall establish policies and procedures that ensure an end-to-end payment transaction. The merchant's policies and procedures should ensure that for card present or face to face transactions, all steps mentioned above under the chargeback handling section are followed in all transactions without fail. For card-not-present transactions address and card security code (CVX2) verifications shall be done regularly. Airlines or merchants who are accepting credit card payments shall have clearly defined policies and procedures to be followed in handling chargebacks, fraud analysis, reconciliation, and adhering to rules and regulations of card schemes and PCI DSS.

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard created by the Payment Card Industry Security Standard Council (PCI SSC). It was created to help organizations that process credit card payments to prevent fraud through increased controls on data. The airline is therefore responsible for the security of each distribution channels. The airline industry has particular issue in its extended revenue cycle and the extensive use of third party networks and sales locations (Accelya, 2012).

2.11. Summary and knowledge gap

As indicated in the literature review part of this paper, for centuries, coins, notes and cheques were the only options to make purchases and to transfer money between people and organizations. In Ethiopia, as it is in many developing countries, cash is the main mode of payment. This makes the country to be heavily cash- based economy. However, the cost of cash to the financial system is high and this cost is increasing from time to time. Becasuse of this, modern society is gradually catching the cashless syndrome. E-payments, ATM cards and others are now the order of the day at our work-places and in the market.

The implementation of electronic commerce based on e-cash as the main engine driving global economic activity will determine the future shape of society (Akinola, 2012). The introduction of plastic cards, Electronic Fund Transfer, Internet banking, and pre-paid payment cards all aimed at making payment more efficient. Many of these innovations offer advantages in terms of costs, security, and convenience (WorldPress, 2014). Card-based alternatives to cash payments are now well established, with credit and debit cards in popular usage.

Debit and credit card payments are convenient for consumers, widely accepted by merchants, and more efficient than paper forms of payments. But as cards have become the primary payment instruments in many transactions, card fraud has also been increased. The new innovations also create increased possibilities for processing mistakes and fraudulent transactions that can result in chargebacks (Visa, 2008). As the world moves closer into becoming a global cashless society, fraud also evolves into more sophisticated forms. Understanding the nature of fraud and fraud prevention mechanisms may help decision makers in addressing these issues more effectively (Yogi, 2011).

However, there is limited study on the nature of credit card frauds, their impact and how to prevent or mitigate them. According to UATP's (2014) report on World Financial Symposium 2014, fraud costs the airline industry close to US\$ 2 billion annually,

approximately US\$ 2.4 Million per airline on average. Dara and Gundemoni (2006) studied on “Credit card security and e-payment” focused only on how to stop hacking of credit card details in the card-not-present environment. Especially, in developing countries where awareness of the card payment industry is less, the problem is deep since the rules and regulations of the card schemes during the card acceptance process is not clearly known and the handling of fraud and chargebacks is not as effective as expected. This knowledge gap is, therefore, the main reason for this study.

Even though many prior scholarly researches are conducted on the various aspects of credit card fraud, to the knowledge of the researcher there is no any research which studies the impacts of such frauds on merchants in developing countries and in particular on Ethiopian Airlines. So as per the researcher’s level of understanding it is a crucial time to undertake a research on the topic to assess the challenges of using credit cards to Ethiopian Airlines, to what extent do Ethiopian Airlines’s internal control systems enable the airline to mitigate the fraud risks.

Chapter Three: Research Design

A research design is the logic that links the data to be collected (and conclusions to be drawn) to the initial questions of a study (or a strategy or plan of action that links methods to outcomes) (Creswell, 2003). This study examines and evaluates internal control systems of Ethiopian Airlines pertaining to its credit card sales management and to assess the chargeback handling and card fraud management practices. In another way, the study examines how effective are Ethiopian Airlines' credit card sales management systems. To undertake this research, the study employed mixed method research approach, where the Qualitative approach is the prime method. In this chapter, the researcher discussed the rationale for using the given strategies of inquiry, specific research methods and ways of collecting and analyzing the data.

To examine the credit card sales management practices at Ethiopian Airlines and identify the main problems and challenges, data were obtained using both primary and secondary sources of data. Semi-structured interviews with the airline officials, questionnaires, observations and review of the system and related manuals and procedures were used. Various reports by credit card sales consolidators/acquirer banks about chargeback and fraud rates and analysis relating to Ethiopian Airlines in particular and the industry in general were also used. Specifically, in-depth interviews were held with the following six officers who have direct roles on credit card transactions in different positions at different times.

Surveys of the airline staff at various ticket offices and stations abroad (mainly who are working on ticket sales and airport check-in), and administrative and support staff at head office on the effectiveness of credit card sales management system were conducted from Mid of March 2015 to Beginning of April 2015. These surveys were conducted using semi-structured questionnaires designed to elicit mainly qualitative data on response time and problems in the system. Both surveys are conducted using face-to-face, online and telephone discussions.

3.1. Strategies of Inquiry

The most important condition for differentiating among the various research strategies is to identify the type of research questions being asked (Hair, 2003). There are some situations where all research strategies might be relevant and other situations in which two strategies might be considered equally attractive. We also can use more than one strategy in any given study. To this extent, the researcher believes that the various strategies are not mutually exclusive. But we can also identify some situations in which a specific strategy has a distinct advantage (Yin, 2011)

The researcher therefore, adopted mixed method research approach to examine the effectiveness of the airline credit card sales management system with a view to achieve convergence across qualitative and quantitative methods (triangulating data sources). Therefore, employing this approach was used to neutralize or cancel out the biases (limitations) of applying any of a single approach and as a means to offset the weaknesses inherent within a method with the strengths of the other method (Creswell, 2003).

In addition, adopting of mixed method research approach in this research provides the best understanding of a research problem because it opens the door to multiple methods of data collection and to both generate the findings to a population and develop a detailed view of the meaning of a phenomenon or concept for individuals (Creswell,2003).This research approach poses the researcher to the challenges for the need of extensive data collection, the time- intensive nature of analysing both text and numeric data, and the requirement for the researcher to be familiar with both forms of research (Creswell, 2003).

Concurrent procedure was employed in undertaking this research which, converges qualitative and quantitative data in order to provide a comprehensive analysis of the research problem. Moreover, the researcher collected both forms of data at the same time during the study and integrated the information in the interpretation of the overall results (Creswell, 2003).

3.2. Research Methods

To undertake this research, the specific methods employed were survey, semi- structured interview and document and system review. Credit card sales reports, chargeback and fraud reports, chargeback appeals, policies and procedures were reviewed by the researcher. The researcher also took observation of how the system works from the card acceptance up to fraud management processes.

Surveys mainly for the quantitative strategies were used through distributing self-administered questionnaires to staff of the airline and to payment consolidators who have direct relation with the day-to-day credit card activities and payment and marketing strategy development. Review of sales procedures, chargeback handling, fraud management and reconciliation manuals and procedures was carried out to have full understanding of the system.

3.2.1. Questionnaires

As clearly indicated above, sales agents at the purposely sampled area offices and stations, airports, and staff at administrative offices of the airline head office were included. Questionnaire was distributed to 65 customers who buy air tickets with their credit cards; 60 of the airline staff and 5 staff of the payment consolidators or acquirers. Questions present in the form of affirmative statements, relating to the card acceptance procedures, chargeback and fraud handling and internal control systems in general in such a way to enable measurement of the respondent's opinions. The respondents were asked to indicate their level of agreement on a five point Likert scale with the following ratings: Strongly agree (5), agree (4), neutral or don't know (3), disagree (2), and strongly disagree (1).

The numbers were indicated in the questionnaire to provide a feel of ordinal scale measurement and to generate data suitable for some quantitative analysis. The central issue to argue that Likert scales produce ordinal data is because of no way at all of knowing whether the differences between the different points on the scale are truly equivalent, and

the points on an ordinal scale are not necessary equally spaced as they must be in order for it to be regarded as an interval scale (Hole, 2011).

To draw additional information, the respondents were requested to provide open-ended responses if they have opinions which they feel the researcher would find useful. The questionnaires are developed based on card scheme and card payment industry's rules and regulations and best practices in the card payment industry.

3.2.2. Interviews

In the qualitative strategy, semi-structured interview was employed with 6 directors and officers of the airline (head office only) to have sufficient information regarding the research problem. The major purpose of this interview was to corroborate certain facts that the investigator already thinks have been established (Yin, 1989, p. 89). Therefore, the semi-structured interviews were conducted to enhance and supplement the results of questionnaires. Semi-structured interviews were prepared based on pilot test which conducted with some of the interviewees so as to enhance the internal validity of the instrument.

3.3. Survey Design

Survey design provides a quantitative or numeric description of trends, attitudes, or opinions of a population by studying a sample of that population. Its purpose is to generalize from a sample to a population so that inferences can be made and it is also economical and rapid turnaround in data collection (Creswell, 2003); and this method is important for collecting large amounts of raw data using question and answer formats (Hair, 2002). Survey is conducted via self-administered questionnaire from the purposely sampled sales agents and randomly taken area managers and station managers; for questionnaire is a common place instrument for observing data beyond the physical reach of the observer (Leedy, 2012).

The main advantage of this survey is its ability to accommodate large sample sizes at relatively low costs, ease of administration and ability to tap in to factors that are not directly observable (Hair, 2002). Moreover, the airline is operating in many countries across five continents and it is difficult for the researcher to reach sales agents at all of these airports.

3.4. Sample Design

Survey sampling is the process of choosing, from a much large population, a group about which one wishes to make generalized statements; the selected part shall represent the total group (Leedy, 2012). The airline staff who are working either on ticket sales through credit card, chargeback or fraud handling and accounting of credit card sales; agents who are selling tickets on behalf of the airline, and staff of payment consolidators such as Euroline and WorldPay are taken as population, and the researcher purposely draw a sample of 65 from all these groups to get rich evidence. To undertake this research paper, the researcher purposely sampled staffs that have been working for the airline, the payment consolidator, or the general sales agent at least one year and above to have sufficient and quality responses (please see Table 3 for more information on this).

Sources	Population size	Sample selection criteria	Sample size
Administrative and support staff of the airline	21	Work with ET at least for a year	10
Sales agents of the airline including area and station managers	330	Work with ET at least for a year	50
Payment Consolidators	10	Work with ET at least for a year	5

Table 2: Sample size design

The sampling design for the population is single-stage sampling in which the researcher has access to names in the populations and sampled the airports/stations and agents directly (Creswell, 2003). The procedure used for drawing the sample from the available stations and agents is based on the credit card sales volume and chargeback rates, for the reason that the study is intended to use more valid and relevant sources. Thus, this research paper used purposive sampling method to draw the sample from the population.

3.5. Data Analysis

Data analysis consists of examining, categorizing, tabulating, or otherwise recombining the evidence, to address the initial proposition of a study (Yin, 2011).

The researcher analysed the data collected through survey concerning the current practices and challenges of handling credit card sales by Ethiopian Airlines. The data collected via questionnaires were analysed with descriptive statistics using statistical package for social scientists (SPSS). Furthermore, as cited in Creswell (2003), it is suggested that qualitative research is fundamentally interpretative i.e. the researcher shall interpret the qualitative data. Thus, data collected from the interview and reviews of documents and system is interpreted qualitatively. To sum, the analysis of quantitative data and interpretation of qualitative data combined to seek convergence among the results (Creswell, 2003). The data analysed through SPSS (version 20) and Microsoft Excel were presented using tables, graphs, charts and figures.

Chapter Four: Data Analysis and Interpretation of Results

Introduction

This chapter begins with general background of Ethiopian Airlines and its internal control system over credit card as a payment method. The second section presents the analysis and interpretation of data collected through questionnaire, interview and review of internal control systems and documents on credit card sales and associated card fraud according to protocols established in Chapter 1 and detailed in Chapter 3. The final section presents summary of the chapter.

4.1. General background of Ethiopian Airlines

Established in 1946, Ethiopian Airlines became the most successful and the largest airline in Africa. In spite of the difficulties facing the aviation industry, including escalating fuel prices, the world economy slowdown and fierce competition, Ethiopian Airlines has achieved a record profit in its latest full fiscal year of 2013/14 and has already taken over the leading role from South African Airways since then. Ethiopian Airlines is one of the few airlines that have continued to grow during the past years despite the downturn in the international airline industry. Currently the airline flies to eighty five international destinations covering five continents.

The airline revenue over the last ten years alone has been grown almost by 500% and become Africa's leading and largest airline in terms of its youngest fleet size, annual revenue and number of destinations covered in its wide Network both in Africa and in the World.

In general, the airline is working with a commitment towards its fifteen year strategic plan (Vision 2025) and has already exceeded some of its targets such as passenger number and revenue generated. In April 2015, the airline achieved yet another milestone with the start of its flights to Tokyo, its 85th international destination. By providing the only direct connection between Africa and Asia, Africa and Latin America and the rest of the world its flights play an important economic and tourism ties between the continents (Ethiopian Airlines, April 2015).

Ethiopian Airlines, Africa's largest and most profitable airline has been recently chosen by customers as the 6th most dependable airline in the world according to CBS news. This ranking is based on on-time-performance, average fleet age, and baggage handling services. The airline has been in rapid expansion mode to capture the hot Africa-Asia market. As the airline expands into new markets, to reach more consumers and increase sales, it needs to consider new payment methods, including locally relevant payment types. These so-called “alternative” forms of payment typically have very different fraud and risk profiles to traditional credit card payments. The fraud landscape will be more complex for the airline. Since the internationalization of markets and evolution of purchase channels has opened the door to both revenue opportunities and greater fraud risk.

4.1.1. Ethiopian Airlines Distribution Channels

As indicated in the literature review part of this paper, airlines utilize a broad range of distribution channels and processes to bill transactions. The possible airline distribution channels include direct sales through own sales offices, call centers, direct websites (e-commerce) and indirect sales by means of traditional travel agents, and tour operators. Although the lion's share of its sales are through its direct sales channels, including Citi Ticket Offices, Airport Ticket Offices, call centers, and e-commerce (web sales) Ethiopian Airlines also utilizes the indirect sales channels notably the traditional travel agents

4.1.2. Payment methods used by Ethiopian Airlines

Although there has been a massive growth in alternative payment methods in the last decade, airlines are slowly adopting them into their payment operations to increase sales conversion in countries where credit cards are not commonly available and to reduce their merchant fees (Helldorff, 2014). Since the majority of Ethiopian Airlines operation is in Africa where there is limited banking infrastructure and low payment card penetration, cash is still remain the most important payment method. However, according to the airlines' financial system reports the sales through credit cards is increasing from time to time and currently reaches over 35 percent of the total sales of the airline.

The airline accepts four major international credit cards such as Visa, American Express, MasterCard, and Diners Club. The airline also accepts UATP cards in its sales notably in the USA. Recently the airline finalized the deal with China Union Pay (CUP) and will expand its sales channels and customers convenience especially knowing that the airline operates to four cities in China alone this deal will definitely increase the airlines sales volume.

According the airline revenue systems reports, out of the total sales of the airline around 30% are through the major international credit cards. In terms of card type, transactions in Visa card leads the airline's credit card sales where MasterCard and American Express follow. The following Pie chart displays the contribution of each of the major credit cards that the airline accepts to its total credit sales.

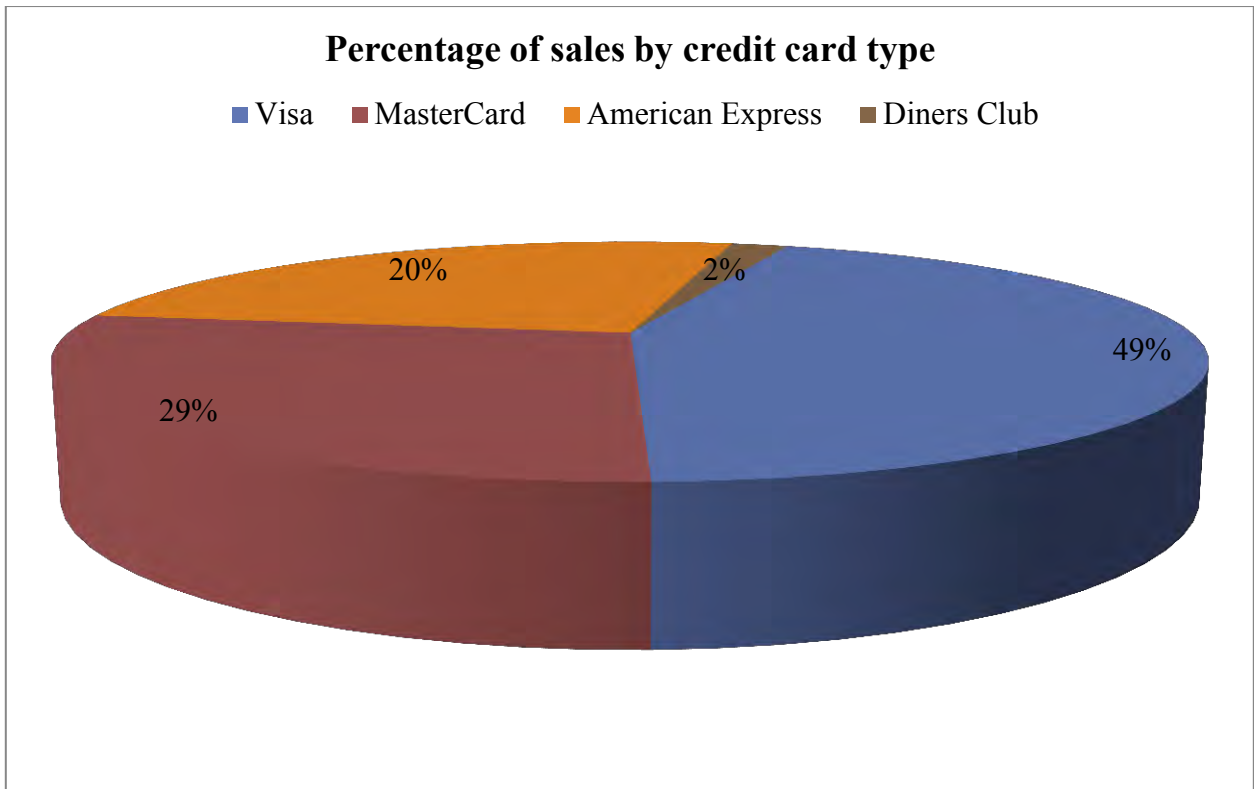
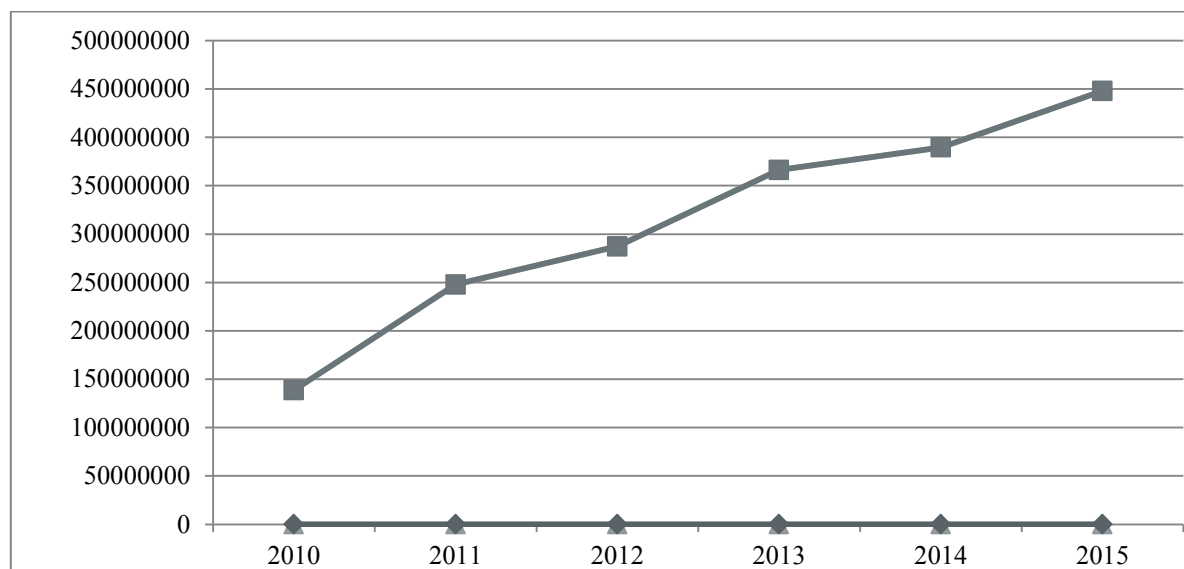


Figure 4: Percentage of credit card sales by card type *(Source: Ethiopian Airlines Financial system reports for 2014/15 Q3)*

As the world is moving to the cash less environment, the proportion of credit card sales of the airline is increasing from time to time. Over the last five years, the airline's credit card sales has increased on the average by 32 percent each year. The below graph shows the growth of credit card sales for the last five years and the year 2015 year to date and eastimatd for the remaining nine months.

Figure 5: Growth of credit card sales over the last five years



Source: Financial system reports of the airline-internal document review

4.1.3. Parties involved in Ethiopian Airlines' credit card sales processes

A typical credit card transaction involves many parties including cardholders (customers), merchant, PSP, acquirers, card scheme and issuing banks. All these parties involve in the case of Ethiopian Airlines credit card transactions. With this „holistic“ view, the schemes are ideally placed to work with the merchant, the airline industry in this case, to help reduce the level of card fraud.

As mentioned above, the airline accepts four international credit card types -Visa, MasterCard, American Express, and Diners Club. While American Express and Diners Club provide the acquiring services by themselves Visa and MasterCard play only the card scheme or network role only. While Sabre is used as a payment gateway or PSP, WorldPay Limited is used as an acquirer to the airlines' credit card transactions through Visa and MasterCard. Ethiopian Airlines therefore, uses an acquirer service for these two card types

where these two card types cover over 78 percent of the airlines credit card transactions sales volume.

4.1.4. Card present versus CNP transactions in the case of Ethiopian Airlines

Through its sales channels, the airline accepts both the card present and card not present transactions. Analysis of documents and sales reports of the airline show that the card present transactions cover the majority of the credit card sales transactions of the airline, although the card not present transactions volume has been increasing from time-to-time, where most of the fraudulent transactions come from the card not present transactions. Analysis of sample chargebacks or card frauds show that over 65 percent are from the card not present transactions and 73 percent of this comes only from call centers (telephone orders).

4.2. Data analysis and interpretations

A total of 65 questionnaires were distributed to Ethiopian Airlines staff who have direct connection to credit card transactions either as sales agent, sales manager, area manager, administrative and technical support or senior directors of purposely sampled ticket offices, area offices and officers from head quarter of the airline and 47 useable questionnaires were collected (72.3 percent response rate). In addition, the researcher conducted interviews with five directors and managers of the airline and has participated on various panel discussions and forums organized with payment service providers such as WorldPay Ltd, Wirecard Technologies GmbH, and Accelya with a view to obtaining best practices and standards on card payment processes and card fraud mitigating initiatives. The researcher also reviewed various internal and external documents and reports on credit card sales and card frauds of the airline to have a holistic picture of the current practices and internal control systems implemented by the airline to mitigate the card fraud risk. The analysis is done based on the theoretical framework the researcher presented in Chapter 2.

Descriptive measures of the major questions response and interviews and document review results are presented in the following sections.

4.2.1. Background information

In terms of educational background more than 78.7% of the respondents have obtained Bachelor degree and above and the remaining 21.3% are diploma and certificate holders.

Table 3: Classification of respondents by education level

	Frequency	Percent	Valid Percent	Cumulative Percent
Diploma	8	17.0	17.4	17.4
Bachelor	30	63.8	65.2	82.6
Valid Masters	7	14.9	15.2	97.8
Other	1	2.1	2.2	100.0
Total	46	97.9	100.0	
Missing System	1	2.1		
Total	47	100.0		

Source: Survey results of Descriptive Statistics -SPSS

According to the results obtained from SPSS (Table 5 below) 71.7% of the respondents are directly involved in the selling of tickets through credit cards and the remaining 28.3% provide support to operational team in terms of analysis, IT and technical support. The analysis further shows that 65.2% of the respondents have over five years of service in a credit card sales related position.

The combination of educational background and year of experience from the analysis shows that the respondents are mature enough and appears to be in a position to provide careful and honest opinions to the questions.

Table 4: Current position and year of experience of respondents

	Frequency	Percent	Valid Percent	Cumulative Percent
ET Sales agent	17	36.2	37.0	37.0
Travel Agent	1	2.1	2.2	39.1
Airport or station manager	1	2.1	2.2	41.3
Valid Area manager	14	29.8	30.4	71.7
E-Commerce staff	2	4.3	4.3	76.1
Finance staff	10	21.3	21.7	97.8
Payment consolidator	1	2.1	2.2	100.0
Total	46	97.9	100.0	
Missing System	1	2.1		
Total	47	100.0		

Year of service in current position

	Frequency	Percent	Valid Percent	Cumulative Percent
1-5 years	16	34.0	34.8	34.8
6-10 years	7	14.9	15.2	50.0
Valid 11-15 years	9	19.1	19.6	69.6
Over 15 years	14	29.8	30.4	100.0
Total	46	97.9	100.0	
Missing System	1	2.1		
Total	47	100.0		

Source: Survey results of Descriptive Statistics -SPSS

4.2.2. Card acceptance and authorization practices

An authorization request is a request to the cardholders issuing bank to authorize a payment transaction that the cardholder would like to perform in return for the goods or services that they are purchasing from the merchant (Helldorff, 2014). Authorizing transactions is a critical step in the credit card transaction process and sales agents shall be careful in sending all relevant and necessary data to reduce the possibility of transactions being returned as fraud or chargeback at a later stage. Upon receiving an authorization request, the issuing bank follows a number of checks to ensure that the transaction is genuine, the card is active, and that the cardholder has sufficient funds to cover the transaction. If properly done, authorizing a transaction is quick and easy, and helps protect merchants against fraud and chargebacks.

Table 5: Agents always request the issuing bank for authentication of the card

	Frequency	Percent	Valid Percent	Cumulative Percent
Disagree	8	17.0	17.4	17.4
Neutral or don't know	12	25.5	26.1	43.5
Valid Agree	17	36.2	37.0	80.4
Strongly agree	9	19.1	19.6	100.0
Total	46	97.9	100.0	
Missing System	1	2.1		
Total	47	100.0		

Source: Survey results of Descriptive Statistics -SPSS

As indicated in the table above and noted from the document review and interviews, sales agents usually request authentication from the issuing bank before accepting credit cards as payment method and executing the transaction. According to the SPSS descriptive statistics results, 56.6% of respondents responded positively (37% “agree” and 19.6% “strongly agree”) that credit card transactions often go through the authorization process. Although 43.5% of the survey result shows that participants either disagree or don’t know

that transactions are authenticated by issuing banks, the document review and interview results indicated that almost all credit card transactions are being authenticated by issuing banks.

Requesting issuing banks for authentication of credit card transactions by itself will not reduce fraud and chargebacks. Sales agents shall continue with the transaction only when an “approved” authorization response is received from the issuing bank. The survey result (Table 7) shows that 61.4% of respondents agree that they accept a valid approval code from issuing banks before they continue finalizing the transactions. Review of the transaction flow and interview responses show that agents that request authentication also obtain approval code before accepting credit cards and executing the transaction. Percent

Table 6: Obtain valid approval code from the issuing bank

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	1	2.1	2.3	2.3
Disagree	5	10.6	11.4	13.6
Neutral or don't	11	23.4	25.0	38.6
Valid know				
Agree	19	40.4	43.2	81.8
Strongly agree	8	17.0	18.2	100.0
Total	44	93.6	100.0	
Missing System	3	6.4		
Total	47	100.0		

Source: Survey results of Descriptive Statistics -SPSS

Transaction authorization is a necessary but not sufficient condition to guarantee payment to merchants. Accordingly, merchants are expected to use state of the art technologies at the time of data entry and sales agents shall use common sense and appropriate caution when

evaluating any customer behaviour or other irregular situation that may occur during a transaction. As indicated in another section of this thesis authorization of a transaction and receipt of an authorization code doesn't guarantee payment (IATA, 2009). Merchants should therefore undertake their own further checks either prior to or after the authorization in order to validate the customer since if the sale turns out to be fraudulent, the full transaction amount may be charged back to them and will even be subjected to some fees.

One of the practices to be done by merchants at the time of card acceptance is to request the cardholder to complete and sign a Universal Credit Card Charge Form (UCCCF) and further request the cardholder to sign this form after duly completed. The study revealed that 57.8% of the total respondents confirmed (37.8% "agree" and 20% "strongly agree") that cardholders are requested to complete and sign this form in addition to obtaining authorization code from issuing banks. However, interview results and discussions with acquirers indicate that request for completion of this form has been reduced from time-to-time.

Table 7: Completion of UCCCF by customers

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	2	4.3	4.4	4.4
Disagree	6	12.8	13.3	17.8
Neutral or don't know	11	23.4	24.4	42.2
Agree	17	36.2	37.8	80.0
Strongly disagree	9	19.1	20.0	100.0
Total	45	95.7	100.0	
Missing System	2	4.3		
Total	47	100.0		

Source: Survey results of Descriptive Statistics -SPSS

Although the survey results showed that customers of the airline are often requested to complete and sign the UCCCF, this method is very traditional and may affect customer's conveniency. Becuase of this and as some countries will not allow merchants to request

customers to complete this form, the practice is being abandoned by many merchants. Instead merchants are expected to implement the latest card technology that can read the card details and send it over to issuing banks for authorization. Best practices show that agents shall keep key-entered transactions at acceptably low levels and use only for exceptional cases when the magnetic stripe or other machines fail to detect details of the credit card. The traditional way of inputting personal account numbers using manual key entry (PKE) has been already replaced by magnetic stripe, point of sales (POS) machines, and lately by Chip and Signature and then by Chip and PIN technologies (put in their order of increased security for merchants). This is because key-entered transactions expose merchants to higher fraud and chargebacks since the possibility of detecting from the card will not be a possibility if data are manually key entered.

The current practice of Ethiopian Airlines shows that most data are inputted using manual key entry and as a result most fraudulent transactions of the airlines come from such key-entered transactions. As shown from the below table most of the selling agents (48.7%) use more of key entry when they input credit card and transaction details for authorization purpose.

Table 8: Agents use less of key entry

	Frequency	Percent	Valid Percent	Cumulative Percent
Strongly disagree	11	26.8	28.2	28.2
Disagree	8	19.5	20.5	48.7
Neutral or don't know	11	26.8	28.2	76.9
Agree	7	17.1	17.9	94.9
Strongly agree	2	4.9	5.1	100.0
Total	39	95.1	100.0	
Missing System	2	4.9		
Total	41	100.0		

Source: Survey results of Descriptive Statistics -SPSS

Since most of the credit card transactions are inputted through the key entry method an analysis of one year (2014/15) card fraud count for the airline shows that over 50% of the card frauds come from the key entered transactions.

4.2.3. Awareness of the PCI and Card Schemes' standards

Whether sales agents are experienced or new to the job, if they follow a few basic card acceptance procedures and standards, they will do it right the first time and every time. Merchants should program their terminals and arrange recurrent training for their operational and back office staff so that sales agents can follow the prompts and properly process the transaction (Visa, 2014). Security of credit card and other personal customer information is of paramount importance for the security of customer information and the integrity of the credit card process.

In order to prevent the fraudulent use of card account number and expiry date and to strengthen data security, the International Card Schemes have introduced a standard, known as the Payment Card Industry Data Security Standard (PCI DSS), that is applicable to all merchants. Compliance with this standard is mandatory, in order to protect all card account information that is processed, stored or transmitted by any entity regardless of the merchant sector. All airlines and travel agents that process credit card transactions are therefore required, in the interests of securing their own data security and to avoid penalties imposed by the card schemes and above all to maintain customers' confidence that cardholders data will be kept secured and to comply with PCI DSS (IATA, 2009). In a recent attempt to move the air transport industry into the age of PCI-DSS compliance IATA has also established the PCI-DSS work group to develop proposals, recommendations, and implementation plans and guidelines that are compliant with the PCI standards (IATA, 2009). The airline is therefore, responsible for the security of each of its distribution channels and PCI compliance is mandatory for the industry.

In general, processing payments is governed by several layers of laws, rules, standards, and compliancy regulations. The card schemes, governments and the airline industry all have their own say on payment processing and standards (Helldorf, 2014). Awareness of such rules and standards and full compliance to them will help merchants avoid unnecessary costs and maintain customers loyalty in this era of cashless enviroment. In an attempt to this the researcher produced some questions to survey participants, reviewed manuals and discussed with higher officers. The survey results show that many of the operation and back office staff of the airline are not aware of these rules, regulations and standards. Moreover, there is no written manual and well-organized recurrent training provided to these staff to develop their awarento ess and enable them strictly follow the rules. Below are the reults of the survey.

Table: 9 Awareness of rules, regulations and standards and existince of adequate training

Questions	% Responses				
	Strongly disagree	Disagree	Neutral or don't know	Agree	Strongly agree
Staff knows about PCI DSS	2.6	28.2	48.7	10.3	10.3
Agents maintain records safely per CPI DSS	0	17.5	45.0	17.5	20.0
Staff are aware of what is expected of them	5.0	27.5	17.5	22.5	27.5
Sales agents know that they are the first person to protect fraud	-	32.5	22.5	22.5	22.5
ET has a knowledge sharing system	7.3	56.1	22.0	12.2	-
Adequate recurrent training for operating and back office staff on card acceptance and fraud handling	42.5	20.0	17.5	15.0	5.0

Source: Survey results of Descreptive Statistics -SPSS

The study revealed that almost 80% of the respondents either don't know about the PCI DSS or some respondents don't agree that front line employees of the airline don't know about the standards and that means there is no compliance to the standard and records and data are not maintained per the standard. Document review and interview discussions confirmed that there is no manual or guideline established for agents to refer at time of or after the transaction is executed. This practice appears to expose cardholders to insecurity and the airline will be subjected to card fraud. The study further revealed that staff are less aware of what is expected of them, they don't know that they are the first person to mitigate card fraud, and the lack of knowledge sharing system worsens the case.

Although the airline has a well-organized aviation academy with various recurrent and leadership trainings, there is no training provided to sales agents and back office staff of the airline to make them aware of the various rules, regulations and standards governing the payment card industry and to discharge what is expected of the airline as a merchant. 62.5% of the respondents confirmed (42.5% "strongly disagree" and 20% "agree") that there is no adequate recurrent training and 17.5% of respondents remained side-lined. Even though 20% of the respondents agree on the existence of adequate recurrent trainings, only 12.2% of the same respondents agree on the existence of knowledge sharing systems. Review of documents and interviews results showed that there is no or little training provided to staff on credit card related issues and some of the interviewees boldly advised the researcher that had the airline provided such trainings, the card fraud rates and associated revenue losses of the airline would have been avoided or significantly reduced.

4.2.4. Fraud prevention and management

While fraudsters are getting access to more sophisticated methods to gain access to credit card information and perpetrate fraud, technological advancements in preventing fraud have started showing some promise to combat fraud. Fraud detection technologies enable

merchants to perform highly automated and sophisticated screenings of incoming orders, flagging suspicious transactions while the order is being processed. While none of these tools and technologies can, by themselves, eliminate fraud, each technique provides incremental value in terms of detection ability. As it will be discussed later, best practice implementations often utilize several, if not all of the tools discussed here (ClearCommerce Corporation, 2001).

According to review of relevant documents by the researcher and interview results, the airline uses fraud prevention and screening tools only for its web sales. However, e-commerce transactions constitute a very few percentage of the airlines' transactions and sales in most of the airline sales channels such as MOTO, ATO, STO and others that constitute the lions share of the credit card transactions are left insecured. Survey results show that 51.3% of the repondents in all sales channels of the airline often request cardholders for their billing addresses and send AVS to issuing banks as part of the authorization request.

AVS validates the billing address information provided by the consumer against the billing address information that the issuer has on record for the account. Although the AVS response provides useful information for the merchant to determining the risk level of an order, it suffers from several limitations that make it a weak screening tool if used alone. AVS is not much useful in case of international transactions since it only validates the billing address but fraudsters who obtain billing addresses can still pass the AVS check, and ship fraudulent orders to a different address (ClearCommerce Corporation, 2001). After exporting the data from SPSS to Excel in order to produce a friendlier graphical user interface, the below table and graph were produced.

Table 10: Descriptive statistics for fraud prevention policies, procedures and screening tools

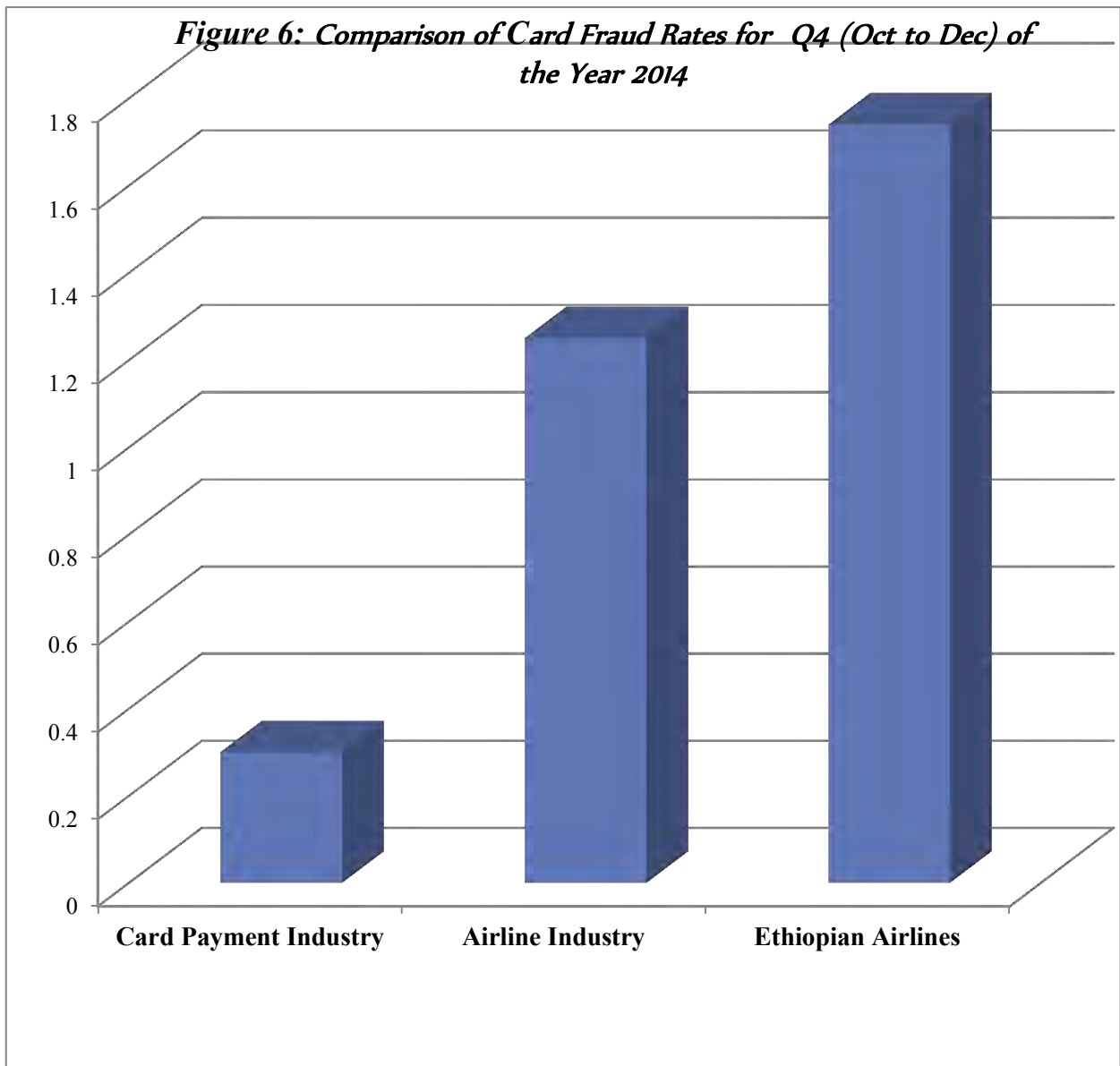
Questions	% Responses				
	Strongly disagree	Disagree	Neutral or don't know	Agree	Strongly agree
ET has clear and effective management policy to mitigate card fraud	5.1	48.7	23.1	17.9	5.1
ET has effective fraud prevention procedures	12.2	46.3	24.4	14.6	2.4
ET has fraud screening tools to all of its sales channels	4.9	39.0	29.3	19.5	7.3
Agent often include AVS in the authentication request	-	20.5	28.2	41.0	10.3

Source: Survey results of Descriptive Statistics -SPSS

Further analysis also showed 56.15% respondents’ disagreement (8.65% “strongly disagree” plus 47.5% “disagree”) on the existence of clear and effective management policy and procedures to prevent card frauds suggesting thereby improvements to mitigate the current increasing fraudulent transactions. Similarly, survey data related to *perceived fraud screening tools* showed that only 26.8% (19.5% “agree” plus 7.3% “strongly agree”) of the respondents supported the overall proposition that the fraud prevention policies, procedures and tools of the airline appears to be weak.

Further analysis of documents confirmed that there is no effective fraud prevention policies, procedures and tools implmented by the airline. Best practices show that many airlines use various fraud screening tools into all of its sales channels and are able to reduce their respective fraud rates to the possible low levels. Both the questionnaire results,

interviews and document reviews showed that Ethiopian Airlines use fraud screening tools such as velocity checking, geo-location checks and verified by visa only to its web sales and none to the other sales channels. As a result the airline appears to be far at risk than both the card payment and airline industry averages which are 0.3% and 1.5% respectively.



Source: CAPA- Center for Aviation Fraud Costs of Airlines & Ethiopian Airlines documents

Although global networking presents as many new opportunities for criminals as it does for businesses, the good news is that technology for preventing credit card frauds is also improving many folds with the passage of time and there are various fraud protection tools that enable merchants to be notified of suspicious transactions, provide a more secured method of authenticating the cardholder at time of transaction and can analyse a fraudulent transaction in a matter of fraction of a second. Since the airline does not use these tools in its major sales channels, the number of fraudulent transactions increases from year to year.

In general, the card fraud level in the airline's sector is disproportionately high. According to Visa's payment card fraud guide for airlines (2014), for example, at two of Europe's „flag carrying“ airlines, fraud rates in 2013 showed in excess of 60 basis points – which is around 13 times higher than the Visa overall average fraud rate for the card payment industry. That means for most airlines, the rates tend to be much higher, particularly through the unsecure e-commerce channel. Digging deeper the fraud rates by channels, by geography, and by the nature of cards (card present versus card not present losses) would enable airlines to initiate appropriate fraud mitigating programmes and to implement fraud preventive tools.

One way of looking at fraud is to consider the location of customers (and the country in which their card has been issued). It is useful to understand that different issuer markets contribute different levels of fraud to the airline business, with different underlying rates. Looking at the total fraud incurred by airlines for the year to September 2013, we can see the main issuer percentage split based on the country where the card was issued as indicated in the below table:

Table 11: Fraud rates by geography of card issuers (card issuing country)

Country where card was issued	Fraud rate by card issuing country
Canada	190 bps
United States	126 bps
France	48 bps
Germany	29 bps
United Kingdom	12 bps

Source: *Managing payment card frauds – a guide for airlines by Visa, 2014*

The researcher used fraud reports by acquirer banks to the airline and made geo-location analysis for using one year card fraud counts for card sales with Visa and MasterCard, which constitute about 78% of the total credit card sales of the airline. The analysis showed that over 70% of the fraudulent transactions during this one year were from cards issued by banks in the United States and Canada.

Country of card issuing banks	Fraud count by country of card issuance
United States	1210
Canada	776
The rest of the world	828

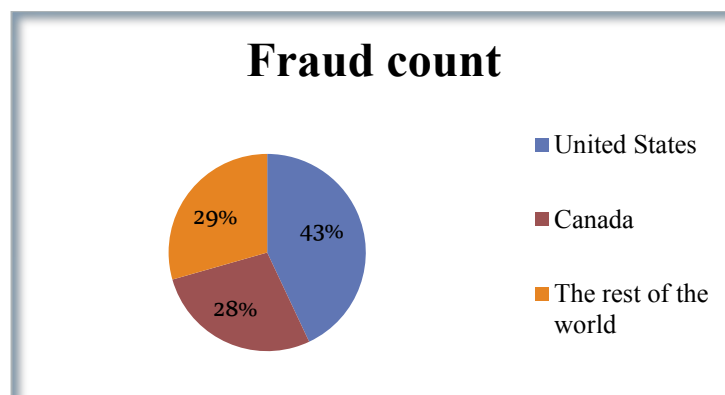


Table 12: Card fraud count by location of card issuing banks (Source: *WorldPay -Acquirer bank's report*)

Ascertaining the location of customers is not conclusive by itself. If the majority of the airlines' sales also were to USA and Canada -based cardholders, we wouldn't be surprised if the majority of the fraud also emanated from these countries. The fraudulent transactions from cards issued in these two countries appears to be to the highest side as compared to that of the rest of the world mainly because the card payment industry is matured in these countries and the card application and issuance procedure may be very easy and not rigorous enough to filter fraudulent applicants leading some applicants easily acquire credit cards with falsified information (with personal information obtained illegally from another individual) and then commit fraud with that card.

When combined with other fraud screening tools like negative and positive lists, understanding cardholders' locations would provide a good indication to merchants to design and implement appropriate fraud prevention tools. A negative list is a database used to identify high-risk transactions based on specific data fields. An example of a negative list would be a file containing all the card numbers that have produced chargebacks in the past, used to avoid further fraud from repeat offenders. Similarly a merchant can build negative lists based on billing names, street addresses, emails and internet protocols (IPs) that have resulted in fraud or attempted fraud, effectively blocking any further attempts. A merchant could create and maintain a list of high-risk countries and decide to review or restrict orders originating from those countries. Both survey results and review of documents by the researcher showed that Ethiopian Airlines does not maintain either negative or positive lists from its chargebacks.

Understanding the nature of card losses by card present versus card not present helps airlines to understand how risk differs, based on the way airlines and their partners process their transactions and also help take appropriate remedy actions. Review of documents by the researcher showed that frauds due to card not present (CNP) transactions are increasing from time to time and disproportionately to the increasing volume of CNP sales. Comparison of card frauds due to CNP transactions with breakdown of three fraud types

MOTO, secure electronic commerce and unsecure electronic commerce are shown in the below table.

Table 13: Comparison of % of card fraud for CNP transactions by of sales channel.

CNP Channel	% of Fraud by Channel	
	Other Airlines	Ethiopian Airlines
Mail/Telephone Order (MOTO)	32%	76%
Secure e-commerce (VbV)	14%	5%
Unsecure e-commerce	54%	19%

Source: Managing payment card frauds – a guide for airlines by Visa, 2014 and Ethiopian Airlines internal documents review

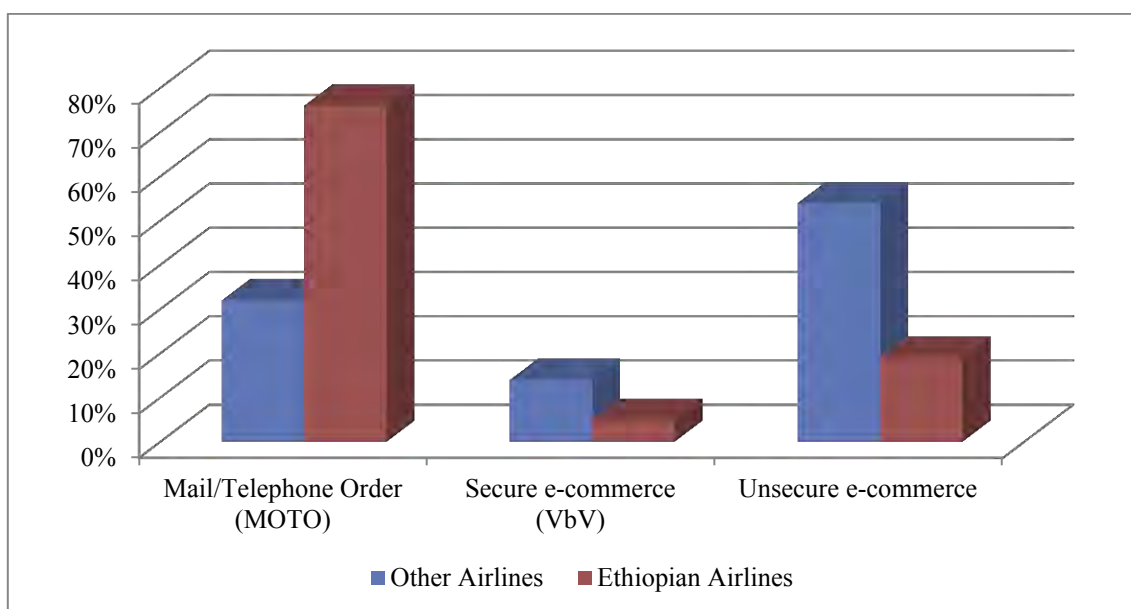


Figure 7: Histograms for volume of card frauds by sales channels (*Source: Managing payment card frauds – a guide for airlines by Visa, 2014 and Ethiopian Airlines internal documents*)

As one can easily see from the table and the graph above, the majority of CNP loss to other airlines occurs through unsecure channels and most of this is unsecure e-commerce. It is also notable that the underlying fraud rate within VbV secured transactions is far lower than the unsecure channels. A merchant that supports VbV can normally expect a full payment guarantee in the event of fraud. Ethiopian Airlines e-commerce frauds are lower than that of the other airlines since the airline sales volume through web sales is still at its early stage and covers only a small proportion of the total credit card sales volume.

The research showed that the airline doesn't have the appetite to invest heavily in keeping pace with the increasingly complex fraud landscape. The management are painfully aware of the scope of the evolving challenges (the survey result showed that 56.5% of the respondents either strongly disagree or disagree whereas only 28.3% agree or strongly agree on that the airlines' management know the true cost of card fraud. 15.2% of the respondents know nothing about the the managements' awareness of the true cost of card fraud). As a result review of documents by the researcher showed that the airlines' fraud counts and the actual fraud losses has been increasing alarmingly over the last eight years (2007 to 2014), although the fraud rates over same period seems decreasing.

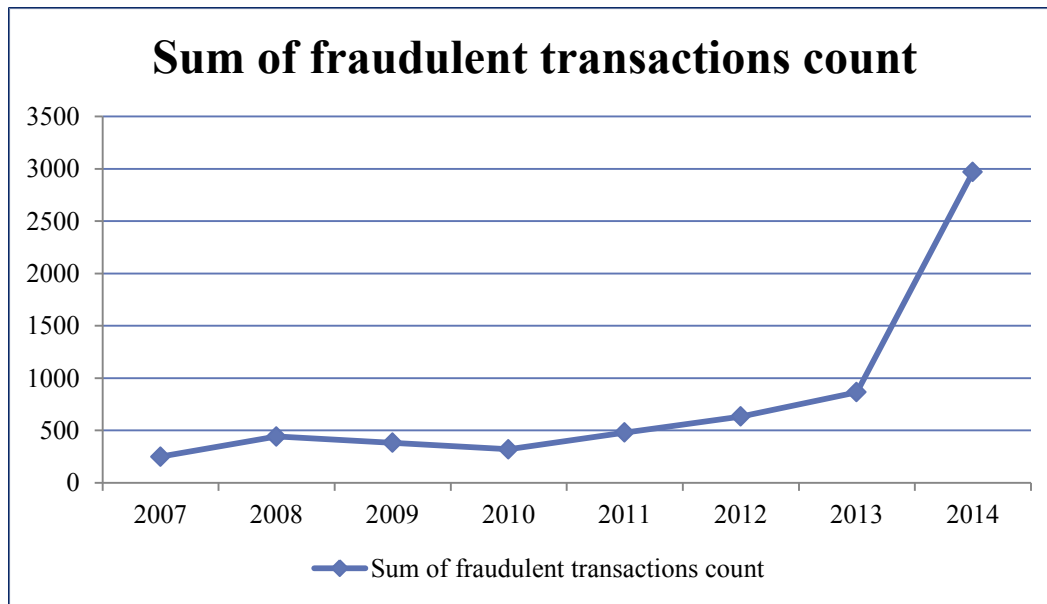
Table 14: Gross sales and fraudulent transactions count for the years 2007 to 2014

Year	Sum of gross sales transactions count	Sum of fraudulent transactions count
2007	34,514	249
2008	91,988	443
2009	107,680	382
2010	145,317	320
2011	184,577	480
2012	213,661	634
2013	271,262	866
2014	390,897	2,971

(Source: Euroline & WorldPay -Acquirer bank's report)

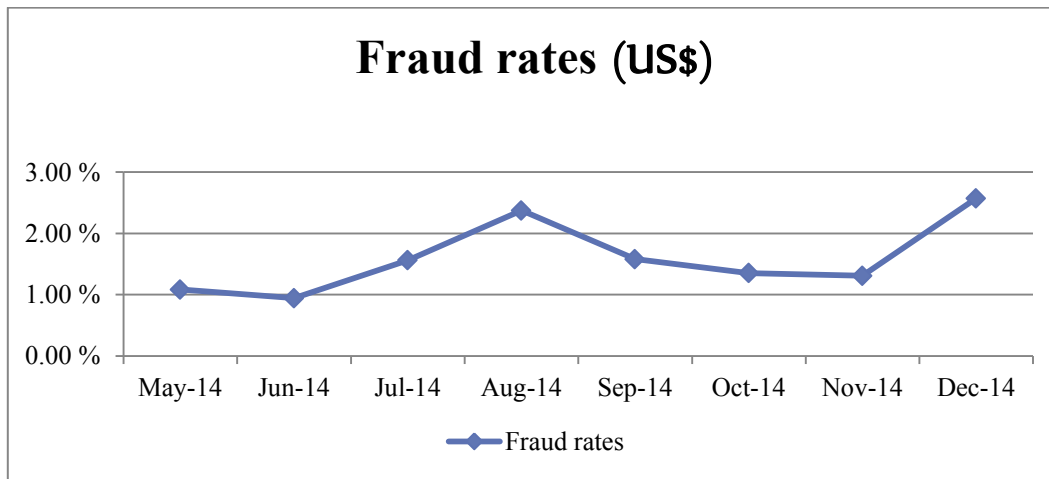
As can be seen from the table above the number of fraudulent transactions has been increasing from year to year and unless the airline takes appropriate fraud preventing tools and procedures the number will significantly increase with the CNP becomes a predominant and growing channel with a disproportionately high fraud rates by nature.

Figure 8: Line chart showing trend of fraud counts over years



The fraud rates over the last eight months to December 2014 also revealed that the airline is losing significant revenue and if it continues this way it becomes a major threat to the airline. Review of reports from acquirer banks showed that due to such high level of frauds the card schemes (Basically Visa and MasterCard) periodically assess and monitor the airline for fraud and chargeback levels, these programmes operate a period of warning and remediation, followed by monthly fines that increase in size if the levels do not reduce, and can lead ultimately to the card schemes revoking acceptance of cards by the airline.

Figure 9: Line chart showing trend of fraud rates over the last eight months to December 2014



Source: *Ethiopian Airlines internal documents review-Monthly report by WorldPay*

4.2.5. Effectiveness of internal control systems of the airline

As clearly indicated in the literature review part of this paper, the use of credit cards as a payment method involves complex processes and a system of trust between many parties, each fulfilling a specific role. The payment process sometimes involves up to eight major participants: cardholders, making a purchase with a payment card, issued by an issuing bank; merchants accepting card payments for good and services that the cardholder wishes to purchase; the acquiring banks, payment processors, payment service providers, and the card associations (card schemes), as well as their respective clearing houses (Helldorff, 2014). Electronic terminals and latest card acceptance devices make transaction processing automatic and seemingly effortless, raising potential profitability. However, they also create increased possibilities for processing mistakes and fraudulent transactions that can result in copy requests and chargebacks.

Airlines are more sensitive to fraud losses and particularly susceptible to fraud compared to other industries due to the perishability of seat inventory and margins that make the loss of

even a single seat to fraud painful to recover from. Ideally, airlines either prevent a fraudster from completing a booking, or are able to discover a fraudulent booking in sufficient time to cancel the reservation and resell the seats. Managing fraud well means minimising fraud losses while simultaneously not offending or inconveniencing genuine customers since one of the main element of fraud costs is the revenue loss due to genuine customers will be lost due to ineffective fraud management or by not rejecting valid bookings or cutting off sales too far in advance of a flight to allow time to process manual review queues. Both of these objectives must be met within the constraints of an operating budget for fraud detection and prevention that is appropriate given the size of the problem.

According to CAPA-Centre for Aviation's fraud analysis with airlines experiencing fraud losses in the range of 1-3% (and over USD 14 Billion a year), there are carriers that actually lose or reject 8% to 25% of good orders because either they have no adequate fraud detection and prevention tools or their automated fraud screening methods can't examine booking with sufficient granularity to accurately interpret whether a booking request is fraudulent or not. According to a survey conducted by Deloitte on behalf of the International Association of Airline Auditors (IAAIA) - Airline Fraud Report 2010, 52% of the surveyed airlines had "no system to formally detect and track fraudulent attempts to obtain tickets, and only half of the respondents had a formal system to pick up unusual transactions or suspicious activities." The report revealed that card fraud is costing each airline an average of more than USD 2.4 million annually.

Some carriers are stepping up their efforts to fight the fraud back. They are boosting the staff that tracks crimes and tapping into new technology that can help detect it. But as large airlines tackle the problem, there is growing concern that fraudsters are moving onto smaller carriers whose defences are not yet in place (Jones, 2010). However, it is only the larger carriers that have taken steps against fraud. As a result, smaller airlines are drawing the attention of criminals. "The fraudster is going to go to the places where there is the least amount of fraud protection,"

The card not present (MOTO and internet) have been dominating the payment card industry. Credit card fraud on the internet and has reached a gigantic proportions, and the merchants providing goods and services over the net are suffering tremendous losses through chargebacks. Merchants who offer a product or service online have to take the risk of losing the cost of the product or service, plus the added cost of chargeback fees, and they even face possibility of having their merchant account terminated or revoked by the card schemes if the level of fraud is rising above certain level and if the merchant is not taking remedial actions to reduce the fraud level.

All the above shows that the current business environment demands airlines to invest heavily in establishing and maintaining strong internal control systems, providing reasonable assurance that frauds can be effectively detected and prevented and addressing the problem from a holistic perspective. With airlines generating billions in revenue a year, the loss of a few million dollars to fraud may not seem particularly alarming. However, “it is a crime” and this is probably the most competitive industry where every dollar counts, and every passenger counts. So airlines shall do all that they can to protect both.

In an attempt to understand both the existence and effectiveness of internal control systems of the airline for its sales through credit cards, the researcher brought some questions to respondents during the survey and interviews and also reviews the airlines’ policies, procedures, and other relevant documents and systems. The below analysis shows some of the most important survey results using descriptive statistics-SPSS and modified by Microsoft excel. The policies, procedures, knowledge sharing systems, information systems, roles and tools in this part are in relation to the card fraud prevention and management practices of the airline and don’t refer to the overall systems of the airline.

Table 15: Summary of descriptive statistics for the existing and effectiveness of internal control systems (SPSS)

Questions	% of responses				
	Strongly disagree	Disagree	Neutral or don't know	Agree	Strongly agree
ET has a well-organized credit card office	23.9	34.8	26.1	8.7	6.5
Roles are clearly defined by policy	2.2	48.9	28.9	13.3	6.7
ET has a knowledge sharing system to educate its staff	8.7	58.7	21.7	10.9	-
ET has fraud screening tools to all of its sales channels	6.4	38.3	27.7	21.3	6.4
ET has effective fraud prevention procedures	14.9	48.9	21.3	12.8	2.1
ET has clear and effective management policy to mitigate card fraud	6.7	48.9	22.2	17.8	4.4
There are efficient and user friendly information system	26.1	28.3	28.3	10.9	6.5
ET regularly monitors the financial risks due to card fraud	10.6	38.3	29.8	14.9	6.4

Source: Survey results of Descriptive Statistics –SPSS

Analysis of the survey results (in the above table) shows that overall 55.6% of respondents on the average expressed their disagreement (12.4% “strongly disagree” and 43.2% “disagree”) on the existence and effectiveness of policies, procedures, systems, and tools to detect and prevent frauds. This in turn clearly shows that the internal control system of the airline is not strong enough to tackle and mitigate the ever increasing card fraud and is not suitable to the environment where the airline industry stands today. Further analysis also showed a 58.7% respondents’ disagreement (23.9% “strongly disagree” and 34.8%

“disagree”) on the existence of a well-organized credit card office that navigates the payment card environment, closely and regularly monitors the trend and new developments in the industry, and effectively liaise operating staff with back office staff and with senior management of the airline.

Further review of documents and interview with officers revealed that the airline is short of well trained and experienced staff equipped with the latest fraud screening, detecting and preventing tools and methods. As indicated in the previous sections of this paper, credit card transactions processes are very complex by nature and when it comes to the airline industry the complexity may probably be twofold of the other sectors. This means the process by nature and the ever changing fraudsters’ techniques demand a vibrant credit card desk with sufficient number of skilled and well-trained experts. Review of documents and interview results showed that the airline has only two payment experts that work with three acquirer banks, reconcile sales against settlements, and review and report fraudulent transactions and respond to chargebacks raised from sales made by both with the airline direct sales and through travel agents in all eighty five area offices and at Addis Ababa. There are also only three fraud experts, analysing the fraudulent transactions and that is basically only for online sales which constitutes a few percentage of the total credit card sales of the airline. None of these (both finance and fraud experts) have taken training on card acceptance and fraud prevention procedures.

Despite the complexity of card payment processes and the ever increasing global card fraud rates the airline seems to give little or no attention to the subject. Although the management of the airline are well experienced and leading the airline into a new chapter they are not on the ball when it comes to credit card fraud. It appears that they are even not aware of the volume of chargebacks and fraud rates. Further analysis of survey results revealed this in that 56.5% of respondents expressed their disagreement (2.2% “strongly disagree” and 54.3% “disagree”) to the question whether the airline management know the true cost of

card fraud to the airline and practical observation by the researcher is even beyond that level of response.

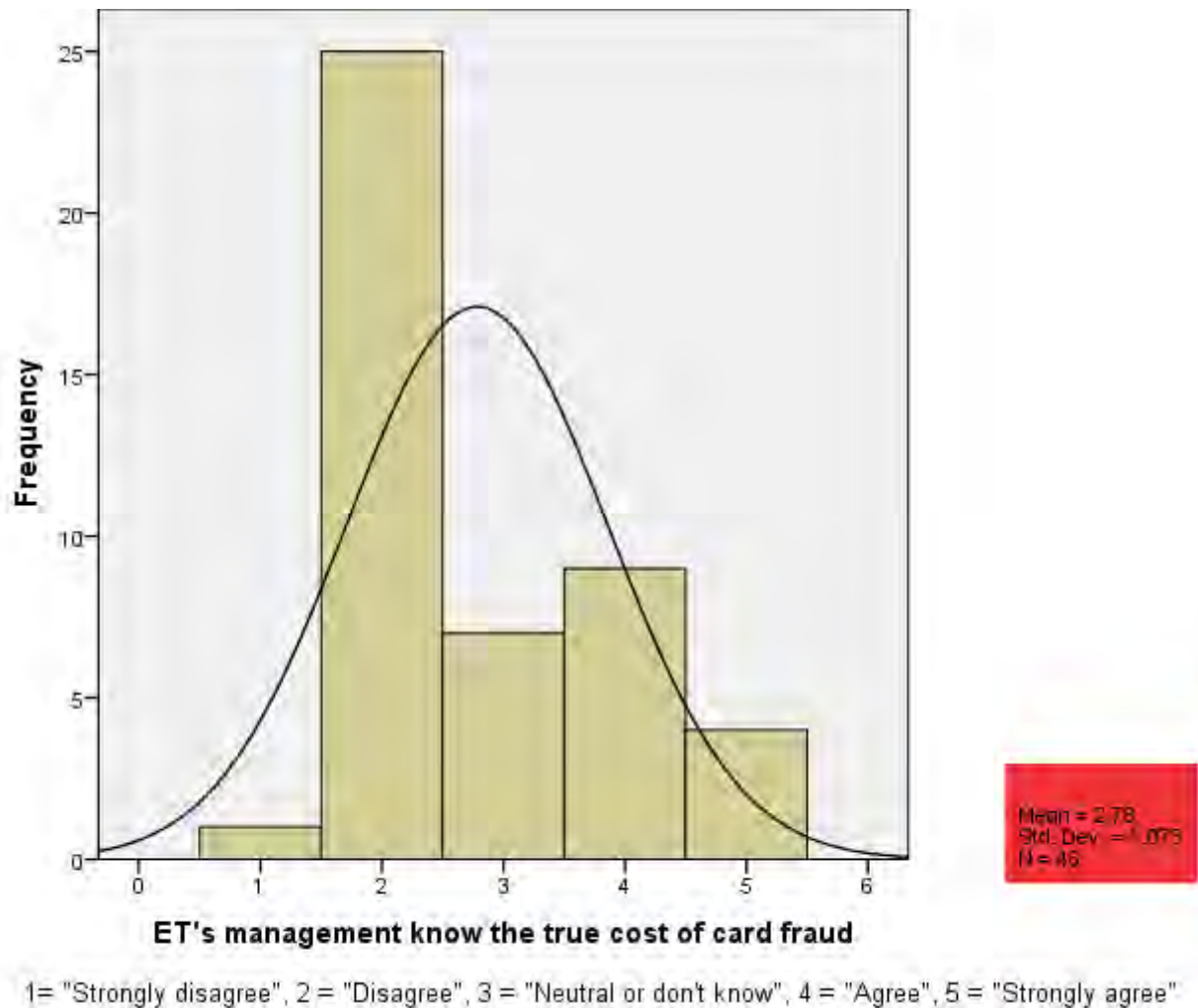


Figure 10: Histogram on ET's management knowledge of the cost of card fraud (*Source: Survey results- Descriptive statistics SPSS*)

A robust management information system (MI pack), which combines current performance and trends, should be critical to everything businesses do. Without strong data, reported very regularly (ideally daily and weekly) and showing the core trends in fraud performance, you are like a hunter wearing a blindfold: you can hear the ducks all around you, but hitting one will be a question of luck – and luck is not something a fraud manager ever wishes to rely upon. Although some of the data may take a while to fully mature, and must always

include trend data, your MI pack will provide a daily overview the basic details needed to monitor the fraud (Visa Europe, 2014). Only 17.4% of respondents expressed their agreement (10.9% “agree” and 6.5% “strongly disagree”) on the existence and effectiveness of the information system suitable to provide the relevant data and enable experts monitor and analyse the fraud trends. While 54.3% of respondents either disagree or strongly disagree on the existence of systems the other 28.3% of respondents know nothing or remain neutral to this. The lack of such strong and robust system coupled with the under resourced credit card office forces experts to engage only on daily fire fighting activities (as the interview the researcher conducted revealed). It is not therefore, surprising if the management of the airline are not aware of the true cost of card fraud to the airline. Most operating and back office staff of the airline even don’t know that card fraud is one of the major threats to businesses today. Further analysis of survey results showed that 27.7% of respondents either disagree or do not know (12.8% “disagree” and 14.9% “don’t know”) about the level of card fraud and how painful it is for businesses today.

The level of respondents’ agreement (20%) on the existence of policies that clearly define roles on fraud analysis is statistically insignificant compared to the level of disagreement (51.1%). It is therefore reasonable to conclude that the lack of clearly defined roles and responsibilities between the different divisions of the airline (Commercial, Financial, and IT) on chargeback handling and fraud management and the complexity of the relationships between the airline and its partners (primarily acquirers, GDS and travel agents) can create certain blind spots – which become a breeding ground for fraud.

To obtain more support and validate the results of the operations performed above, the researcher further analysed responses to the overall effectiveness of the internal control systems of the airline over its payment card processes from card acceptance to fraud management. The result showed that 67.6% of respondents perceive that the system is ineffective (with 27% “very weak” and 40.5% “weak”).

Table 16: Overall ET's internal control system rating

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very weak	10	21.3	27.0	27.0
	Weak	15	31.9	40.5	67.6
	Average	4	8.5	10.8	78.4
	Good	6	12.8	16.2	94.6
	Very good	2	4.3	5.4	100.0
Total		37	78.7	100.0	
Missing	System	10	21.3		
Total		47	100.0		

Source: survey results –SPSS

In summary survey results supported the overall proposition that the internal control system of the airline is ineffective or weak to identify, detect, and prevent card frauds which has been again proven with observation and the high fraud rates of the airline.

Chapter Five: Summary of findings, Conclusion and Recommendation

The primary purpose of this research was to examine the internal control systems of Ethiopian Airlines in relation to card fraud with a view to reduce revenue losses. And the discussions held throughout this paper support the researcher's claim that if Ethiopian Airlines can't strengthen its internal control systems over card acceptance and chargeback and fraud management, it is experiencing significant amount loss of its revenue. Unless effectively dealt with, Card related fraud can affect EAL's bottom line as a result of the revenue loss due to card fraud, loss of reputation, fines and ultimately card schemes can revoke its right to sell in credit cards.

This section of the thesis presented the summary of findings, conclusions and finally recommendations for system improvements and for further researches.

5.1. Summary of findings

A total of 65 questionnaires were distributed to Ethiopian Airlines staff whose day-to-day activities are related to sales transactions made through credit cards either as sales agent, sales manager, area manager, administrative and technical support or senior directors of purposely sampled ticket offices, area offices and officers from head quarter of the airline and 47 useable questionnaires were collected (72.3 Percent response rate).

In addition, the researcher conducted interviews with five directors and managers of the airline and has participated on various panel discussions and forums organized with payment service providers such as WorldPay Ltd, Wirecard Technologies GmbH, and Accelya with a view to obtaining best practices and standards on card payment processes and card fraud mitigating initiatives. The researcher also reviewed various internal and external reports, manuals, procedures and also made observation of card acceptance and fraud management systems of the airline.

Accordingly, data collected through all the three methods (questionnaire, interview and system and document review) were analysed and presented in chapter four. The analysis showed that all three methods produce similar results and they complemented with each other. The results showed that sales agents ensured that credit card authorization is done and an approval code is obtained from issuing banks for each and every sale made through credit cards before they accept the card. This is the first and most important step in the credit card acceptance process. However, authorization and approval by the issuing bank is just a necessary but not sufficient condition to guarantee settlement of transactions made through credit cards.

Accordingly, the sales agents shall take further necessary steps and use latest technologies to screen, detect, and prevent frauds from the first stage. However, the analysis showed that sales agents are not aware of that receipt of an approval code from issuing banks is not a guarantee for settlement of transactions. The analysis further showed that the airline is not using fraud screening and fraud detection techniques and tools for most of the sales channels that cover over 90% of the total credit card sales of the airline. Although technological advancements in preventing fraud have started showing some promise to combat fraud and some fraud detection technologies that enable merchants to perform highly automated and sophisticated screenings of incoming orders, flagging suspicious transactions while the order is being processed, the airline is using none of these techniques and tools in most of the sales channels and as a result the fraud rate of the airline shows increment from year to year and the airline appears to be target for fraudsters.

Credit card transaction processes and card fraud management are very complex activities and demand well trained and skilled experts, tailor made and effective procedures, policies, standards, robust management information systems and strong internal control systems in general. The study showed that the airline does not have well organized credit card department equipped with sufficient and well trained staff, no adequate recurrent trainings to operating and back office staff, no user friendly and well-integrated information system and generally internal control systems of the airline over its credit card acceptance and

chargeback and fraud handling and management are found weak. The study showed that no proper attention is given to the credit card handling department. While the reconciliation and chargeback handling process is being done only by one analyst under the Finance department, the fraud analysis is being done under the e-commerce section under Commercial division. However, there is no proper link between the two sections and there is no clear boundary of responsibility too.

This exposes the airline to excessive fraud and loss of revenue in this very competitive industry where profit margin is very thin. Due to its high volume of chargebacks and card frauds, card schemes especially Visa and MasterCard operate monitoring programmes for fraud and chargeback levels of the airline and these programmes operate a period of (monthly assessments) warning and remediation to the airline. To further illustrate this case, the researcher would like to quote a follow up email from the Senior Relationship Manager of one of the airline's acquirer bank, WorldPay limited, as follows:

*"... I wanted to bring your attention to Martin's email below and the previous emails from our teams to advise of Visa and MasterCard requests for Ethiopian Airlines to address fraud and chargebacks levels that are being recorded. Both card schemes operate monitoring programmes for fraud and chargeback levels, these programmes operate a period of warning and remediation, followed by monthly fines that increase in size if the levels do not reduce, and **can lead ultimately to the card schemes revoking your acceptance of cards.** We have approached the schemes for a waiver and various extensions to their programme requests for information – however we are now in a position where your fraud levels have not yet improved, we cannot demonstrate sufficient details in the appeal documentation to give them comfort that we will see a return to expected fraud levels and **there is a very real threat that you will receive a fine of \$20,000 within this month....**"*

As indicated in the quote above, the airline's fraud losses have been increased from time to time and leading the card schemes to regularly monitor and assess the fraud levels. If the airline does not take corrective actions to reduce the fraud levels the assessment by card schemes will continue and they may even decide to revoke the airline's rights to sell tickets in their respective branded credit cards. While the world is moving to the cashless environment, if the airlines' right to sell in these international credit cards has been revoked by the card schemes, that would be a big problem for the airline despite that the airline shows remarkable growth and success by being the largest and most profitable African airline. WorldPay's report attached to the above message also shows the following comparison of fraud to sales ratio of Ethiopian Airlines with four anonymous airlines over the last one year which shows that Ethiopian Airline fraud rates are to the highest side as compared to others.

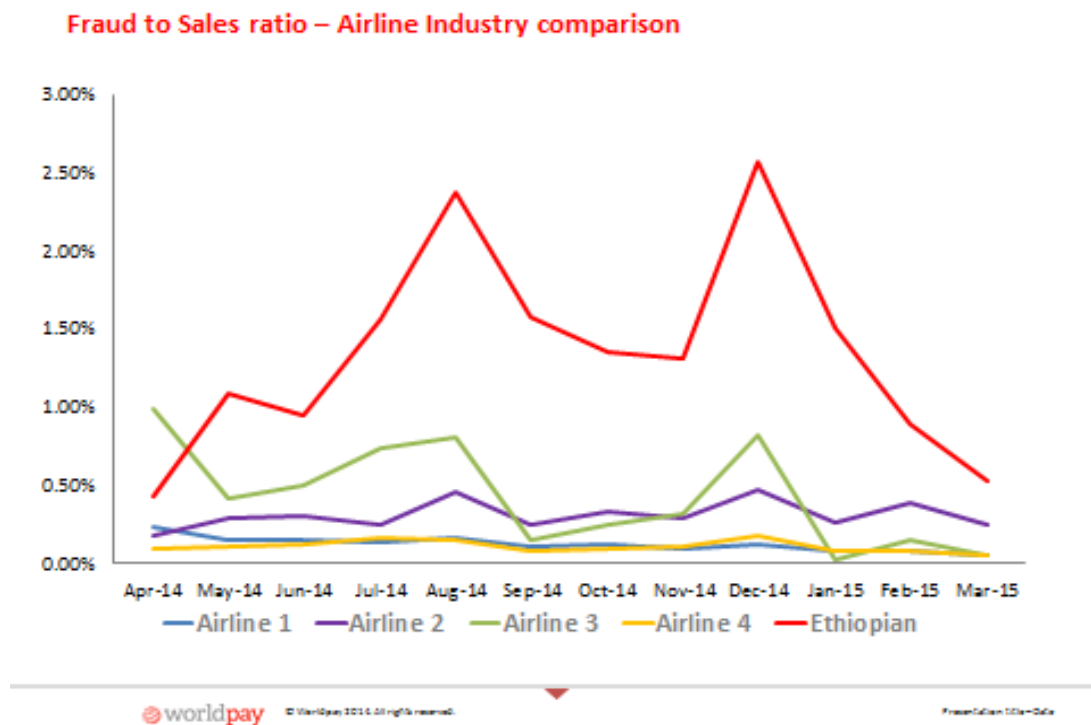


Figure 11: Airline industry comparison of fraud to gross sales ratio (Source: WorldPay's report May 2015)

In general, the research revealed that the airline is seeking comprehensive solutions that account for the ever changing global payments landscape accompanied by multiple fraud schemes or techniques. Specifically, the airline needs credit card risk management solutions that address multiple channels, across multiple payment types, in multiple markets. This research highlights the fact that the airline should consider fraud management solutions that are tailored to its specific business. Moreover, these solutions must be easy to use and simply integrated into existing systems and processes. The airlines' management don't have the expertise to carry out the comprehensive work required to monitor the fraud losses and to provide guidance and necessary support to mitigate the card fraud. Perhaps, partnership with an expert fraud provider is an essential step in reducing the costs of fighting the card fraud, but this does not exist in the case of Ethiopian Airlines currently.

5.2. Conclusion

As indicated in the previous chapters the primary purpose of this research is to examine Ethiopian Airlines' internal control systems over its card acceptance and fraud management practices and to recommend some improvements and further studies on the area.

In order to reach new customers and increase sales, businesses must offer their customers the opportunity to pay in a most convenient way for them. The risks, costs and implications of these payment methods may be significant and in some cases they may tie up much needed capital. On top of this there are more partners to deal with, more players and service companies emerging on the market place, compliance issues, reporting and reconciliation requirements, all in a multi-currency environment where service and reliability are crucial (Lyon, 2008).

As the airline expands into new markets, to reach more consumers and increase sales, they need to consider new payment methods, including locally relevant payment types. These so-called "alternative" forms of payment typically have very different fraud and risk profiles to traditional credit card payments. Cash, cheques, and credit cards were the predominant payment methods used in the airline industry since long time. Although there has been a massive growth in alternative payment methods in the last decade, airlines are slowly adopting them into their payment operations to increase sales conversion in countries where credit cards are not commonly available and to reduce their merchant fees (Helldorff, 2014).

In today's era of information and communication technologies, credit card payments have become simultaneously easier and more complex. Although these technologies make transaction processing automatic and seemingly effortless and raising potential profitability, they also create increased possibilities for processing mistakes and fraudulent transactions that can result in chargebacks (Visa, 2008). Transaction through credit cards may be returned because of rules and regulations violations, because the sale is disputed by a cardholder, or as a result of fraud. There are three basic reasons for a card transaction to be disputed by a cardholder, (1) cardholder can not honor payment (credit risk), (2) cardholder does not

recognize transaction (fraud risk), and (3) cardholder dissatisfied with purchase (Commercial risk) (IATA, 2009).

The first risk is not an issue for the merchant, as card payment is guaranteed with transaction authorization and can be backed by appropriate supporting documents. Liability for the second risk is shifted to the merchant (the airline in this case) especially for card not present transactions if the transaction is not with 3D Secured cards. The third risk should not be confused with fraud as same is a customer service issue. In the past few years, credit card fraud has been one of the most sophisticated crimes in the world. Various prevention initiatives have been employed to prevent this offence and yet global payments fraud statistics suggest that more must be done to address the problem.

Credit card fraudsters employ a large number of modus operandi to commit fraud (Bhatla, 2003). Increasingly, the card not present scenario, such as shopping on the internet poses a greater threat as the merchant (the web site) is no longer protected with the advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the “physical world” checks necessary to detect who is at the other end of the transaction (Bhatla, 2003).

Accepting payments in the travel industry has become increasingly more expensive due to the rising costs of transaction fees and related charges. Airlines pay more than US\$ 7 Billion annually to process card payments (Kaiser, 2014). According to UATP’s (2014) report on World Financial Symposium 2014, credit cards have the highest cost per transaction and airlines pay an average of US\$ 12.50 per ticket for credit card processing and fraud costs the airline industry close to US\$ 2 billion annually, approximately US\$ 2.4 Million per airline on average. Airlines therefore, need to select the right set of methods of payment to target new customers and new markets. Airlines need to align their channel strategy with their payment strategy to drive the sale process. There are new requirements driven by online channels that airlines should pay attention to multichannel, but airlines

also at the same time need to care about all channels, since cards may not lead all of them in the near future (Kaiser, 2014). Effective payment strategies are critical and having the right strategy can significantly reduce cost and potentially provide incremental revenue.

Unlike many other organizations whose operations are limited only to the home country, Ethiopian Airlines operates in five continents, eighty five international destinations and connecting Africa to the rest of the world (Ethiopian Airlines, 2015). Operating globally means it is not an option for the airline not to go out of the traditional payment methods and not to offer convenient distribution channels and payment methods to its customers. Failure to do so gives competitors the cutting edge and enables to snatch customers out of hand.

On the other hand, the management and employees of the airline appear to have limited knowledge and lack awareness of the card payment industry's rules and regulations governing such payment methods. In the writer's opinion this knowledge gap exposes the airline to higher chargeback and fraud losses, penalties by card schemes and may cause revocation of rights of selling tickets through credit cards in the worst scenario. This is the primary reason that motivates the researcher to work in this area. The writer believes that this paper is meant to build more awareness to the airline staff about this growing problem and to offer insights which aid the airline from becoming victim of credit card fraud and to use the card payment method effectively and increase its revenue by developing more effective payment strategy.

The study revealed that the airline sales transactions through credit cards are not supported with the latest technologies and tools that the market offers to detect and prevent card frauds. As a result of this the airline has been exposed to disproportionately higher frauds. The study further revealed that there is no adequate awareness training to operating and back office staff to make them aware of the rules and regulations of the card payment industry and then prevent the airline from excessive card fraud losses and other incidental costs. The lack of robust and integrated information system, lack of well-organized credit

card desk and policies and procedures showing proper assignment of duties and responsibilities across different divisions of the airline in managing fraud makes the overall internal control system for card acceptance and fraud management weak.

As various researches made in this area previously showed the airline industry's fraud rates in general are unproportionately high and this is mainly attributed to the nature of the business that demands close monitoring of the market and strong internal control systems.

5.3. Recommendation

The researcher examined and explained several aspects of the airline practices in accepting credit cards as a payment method as they relate to the internal control system of the company. The findings of the study revealed that there is a wider gap between the best practices in the payment card industry and that of Ethiopian Airlines in terms of accepting payment cards and managing associated frauds. This exposes the airline to disproportionately higher fraud rates and if it continues this way it will become one of the few major threats to the successful operation of the airline. The lack of adequate and recurrent training to operational and back office staff; lack of knowledge sharing system and less supervision and coaching of follow sales agents by immediate supervisors on credit card fraud risks; lack of well-organized credit card office equipped with educated and well trained experts; the absence of effective fraud prevention tools and systems; the absence of clear, effective, and up-to-date policy and procedure negatively affect the quality and strength of the internal control systems of the airline over its credit card sales and chargeback and fraud management. As a result, the implications of the findings from this study lead the researcher to make the following recommendations.

Firstly, awareness is very important for sales agents as they are the first persons to prevent card frauds and save the airline from unnecessary costs and damages. Accordingly, the airline shall arrange an adequate recurrent training to all of its own sales agents and assigned travel agents that are selling tickets on behalf of the airline. The airline has a well-known aviation academy run by managing director and it is easy to include this training as one of the recurrent trainings provided by this academy. As a member of IATA and working with one of the biggest payment consolidators in the world, WorldPay Plc., the airline can easily arrange and provide this training in partner with these organizations. As part of the recurrent trainings, the airline shall have manuals, procedures and policies that show best practices and the rules and regulations set by the card schemes and the PCI. These training manuals will help sales agents to critically verify cards with fraud

prevention in their mind before they sale tickets and maintain cardholder's details in a safe and secured way.

Secondly, today the market offers various technological advancements in preventing fraud which have already started showing some promise to combat fraud and some fraud detection technologies enable merchants to perform highly automated and sophisticated screenings of incoming orders, flagging suspicious transactions while the order is being processed. The airline therefore, needs to implement these tools in all of its sales channels. There is a cost to the airline to buy and implement these tools and technologies, but the cost to them is significantly lower than the loss resulting from fraudulent transactions. These tools will enable the airline to make geo-location analysis, velocity checking, card verification, making positive and negative lists, picking card details easily from the cardholder and avoiding manual entry of card details which usually exposes merchants and cardholders to fraud.

Thirdly, the study revealed that the airline does not have well-organized credit card desk equipped with sufficient and highly skilled experts and robust management information systems. As the researcher acknowledge elsewhere in this paper, the complexity of the relationships between airlines and their partners, credit card transaction processes and fraud management issues can create certain blind spots – which become a breeding ground for fraud and requires skilled manpower and well-integrated and robust management information system.

Currently, the credit card related activities of the airline are handled in a fragmented and disorganized manner (partly under the Finance division and partly under the Commercial division) with no clear responsibility assignment among the two divisions. The volume of the airlines' sales through credit card (currently estimated to be about 30 to 35% of the total sales of the airline) has been increased from time to time; the market is quickly moving to the cashless environment and alternative payment methods are dominating the market; and

most importantly the fraudulent techniques are increased and changing with the technology and hence so is the fraud losses to the airline industry.

As such the researcher recommends that the airline shall give proper attention to the issue, establish a strong department that handles the whole credit card related activities (setting payment strategies suitable to each market, establish and maintain vendor relationships, ensure compliance to rules and regulations, handling the overall credit card related activities and looking for and evaluating APMs) under the Finance division. The new credit card department shall be led by Head of Credit Card and e-Payment Management, reporting directly to the Chief Financial Officer and shall adopt the structure indicated under Fig. 12 here below.

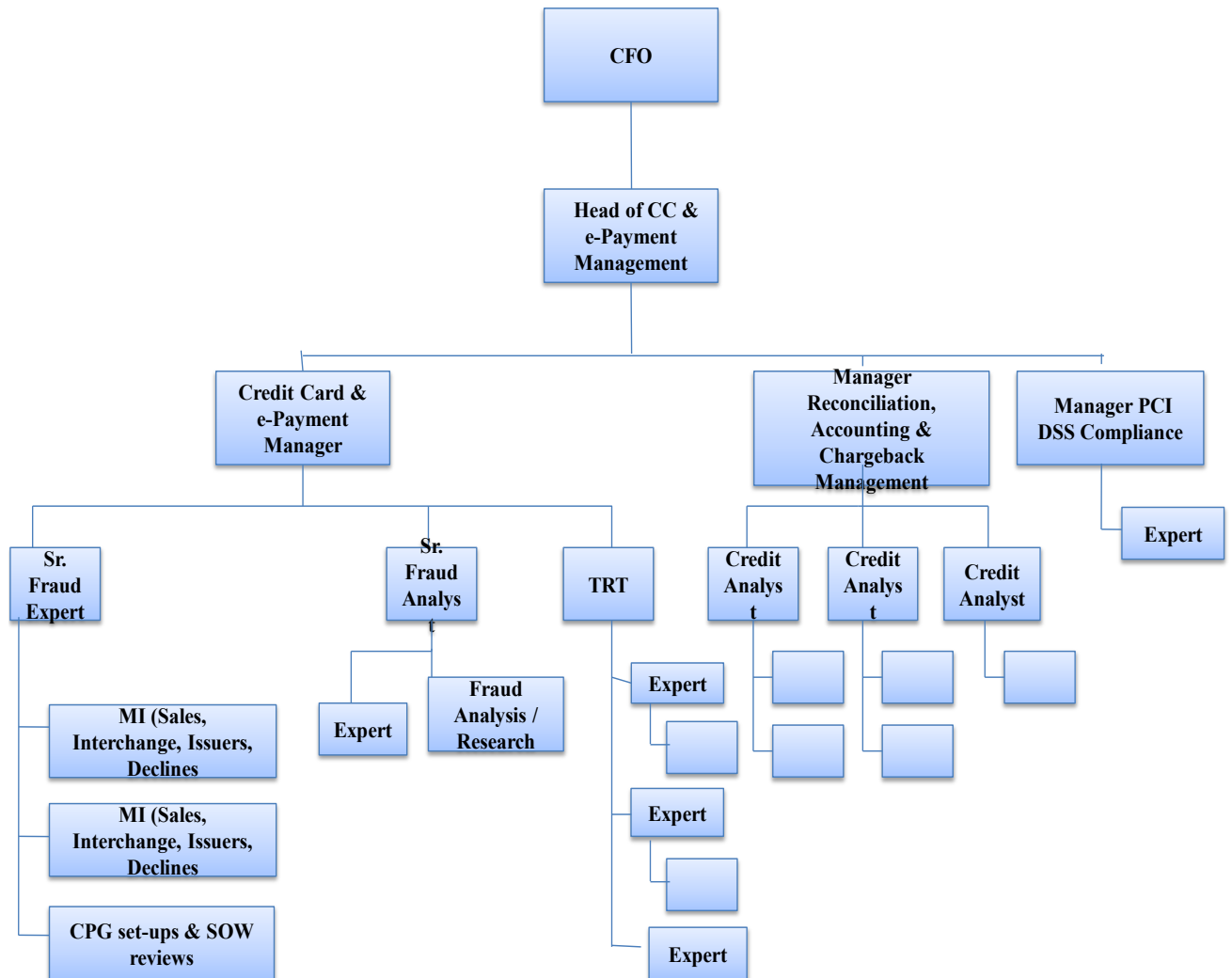


Figure 12 Recommended payment team structure (Source: study of best practices in the industry and own recommendation)

Enhancing the fraud management processes of the airline requires digging the fraud losses deeper by sales channels, by nature of card transactions and by geography or the location of its customers (and the country in which their cards have been issued). It is useful to understand that different issuer markets contribute different levels of fraud to the airline business, with different underlying rates. All these show the need for a great deal of expertise and real time data.

The researcher would like to recommend to the airline to arrange experience sharing with other airlines who are more efficient and effective in the area such as British Airways and Emirates; to arrange especial training for those working on chargeback and fraud management; and to work closely with business partners such as IATA, acquirers of the airline and with credit card organizations. Moreover, the researcher would like to recommend adoption of the following logical but slightly simplified approach (see Fig. 13) of detecting fraud by the fraud experts and the fraud detection system.

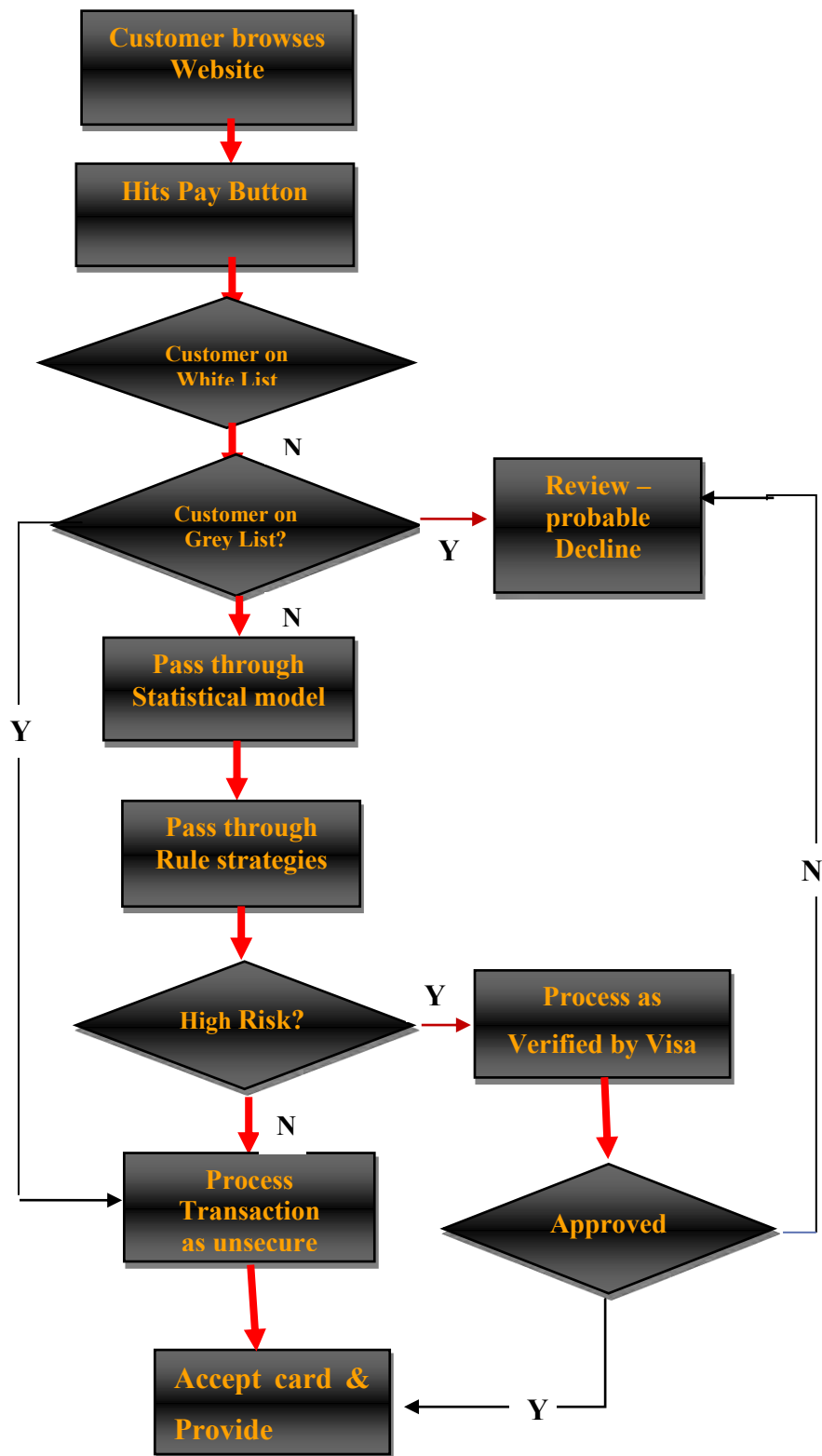


Figure 13: Programme flowchart of fraud detection system (Source:

Fourthly, the researcher would also believe that it is worthwhile checking the airlines' contractual terms with its partners – with acquirers whether their responsibility is only to consolidate payments to the airline or the terms of the agreement obliges the other party to provide fraud management services to the airline and whether it would be possible to pass on chargebacks to GDS and travel agents.

Fifthly, the researcher believes that although the future leader in the airline payment space can still be cards but will need to coexist with alternatives as cards may not lead all of the sales channels in the near future. The airline also adds new destinations every time possibly with a different payment cultures. The airline therefore, needs to select the right set of methods of payment to target new customers and markets. On the other hand the complexity of the new payment ecosystem requires airlines to carefully define their payment strategy. The researcher therefore recommends that the airline shall establish a holistic payment strategy crafted with all its sales channels, markets and customers in mind.

Finally, to the best knowledge of the researcher this paper is the first type written on payment cards and their challenges to merchants with such level of details, at least in the case of developing countries. This study therefore, opens various future research possibilities and can be used as a spring board to take further researches in the area. The researcher did not include experiences of other airlines and would like to recommend future researches to include experiences of at least competitor airlines and also to focus on the challenges and prospects of alternative payment methods.

6. Bibliography

- Accelya. (2012). *Meeting the PCI DSS challenge in airline industry*.
- Akinola, O. S. (2012). Cashless society, problems and prospects. *International Journal of Computer Science and Telecommunications, Volume 3, Issue 8*, 49.
- Bansal, A. (2012). *Challenges & Opportunities for Merchant Acquirers*. Capgemini.
- Bhatla, V. P. (2003). Understanding Credit Card Frauds. *Tata Consultancy Services*, 1.
- Blocher, S. &. (2010). *Cost Management: A Strategic Emphasis 5th ed*. New York: The McGraw-Hill Companies.
- Bruce Rutherford. (2013). *Security Matters*. Retrieved from <http://arm.mastercard.com/securitymatters/technology/emv/best-practices-optimizing-emv-fraud-management/>
- ClearCommerce Corporation. (2001). *ClearCommerce Fraud Prevention Guide*. Texas: ClearCommerce Corporation.
- CreditCards.com. (2015). *Credit card news*. Retrieved January 2015, from The history of credit cards: <http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php>
- Creswell, J. W. (2003). *Research Design; Qualitative, quantitative and mixed methods approaches, 2nd ed, University of Nebraska, Lincoln*. London: Sage Publications, Inc.
- Deloitte. (2010). Airline Fraud Report 2010 - Time to stop the Losses. *Cybercrime*.
- Diners Club, D. (2012). *Company History*. Retrieved January 2015, from <https://www.dinersclubus.com/home/about/dinersclub/company-history?nav=left>
- Drexler, D. B. (2002). Fraud Management in the Credit Card Industry. *Discussion Paper Payments Card Center*. Philadelphia: Federal Reserve Bank of Philadelphia.
- Earnst & Young. (2011). *The digitisation of everything: How organisations must adapt to changing consumer behaviour*. Retrieved January 2015, from [http://www.ey.com/Publication/vwLUAssets/The_digitisation_of_everything_-_How_organisations_must_adapt_to_changing_consumer_behaviour/\\$FILE/EY_Digitisation_of_everything.pdf](http://www.ey.com/Publication/vwLUAssets/The_digitisation_of_everything_-_How_organisations_must_adapt_to_changing_consumer_behaviour/$FILE/EY_Digitisation_of_everything.pdf)

- Ethiopian Airlines. (2015). *Overview of Ethiopian Airlines: Management of Accounts-February 2015*. Addis Ababa.
- Ethiopian Airlines. (April 2015). *Selamta*-The inflight magazine of Ethiopian Airlines. *Selamta*, 5.
- Gebregiorgis, A. (2011). *Internal Audit Functions and Governance: in Commercial Banks, A Thesis submitted to School of Graduate Studies Addis Ababa University, Degree of Master of Science in Accounting & Finance*. Addis Ababa.
- Hair, B. O. (2002). *Marketing Research within a changing Information Environment, 2nd ed*. New York: McGraw-Hill Higher Education.
- Harteveldt. (2012). *The future of airline distribution: A look ahead to 2017, a special report commissioned by IATA*. Cambridge: Atmosphere Research Group.
- Harteveldt, H. H. (2011). *Looking forward to 2012*. Atmosphere Research Group.
- Helldorf, T. (2014). *Airline Payment Methods: a complete guide to payments in the air transport industry*. London: Payments.aero.
- Hole, G. (2011). Levels of Measurement in psychological research. 7.
- IATA. (2009). Airline card fraud prevention best practice guide.
- IATA. (2010). *BSP Data Interchange Specifications Handbook*. Geneva: IATA.
- IATA. (2011). *Travel Agent's Handbook, Resolution 818g Edition*. Montreal: International Air Transport Association.
- Jones, C. (2010, October 18). *Airlines go on guard against cyber-fraud*. Retrieved April 2015, from phys.org/news/2010-10-airlines
- Joseph F. Hair Jr., R. P. (2003). *Marketing Research within a Changing Information Environment 2nd ed*. New York: McGraw-Hill Higher Education.
- Katherine J. Barker, J. D. (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime*, 399.
- Leedy, P. D. (2012). *Practical Research: Planning and Design 10th Ed*. New York: Pearson.
- Lyon, C. (2008, December). *Realex Payments*. Retrieved January 2015, from The real time payment exchange: www.realexpayments.com

- Mason, D. K. (2008). *Air Transport Management Seminar*. Lisbon: Cranfield University.
- MasterCard. (2011). Best in class fraud management: Five MasterCard Recommendations. *MasterCard Academy of Risk Management*, 18.
- MasterCard. (2011). *Company Milestones*. Retrieved December 2014, from http://www.mastercard.com/us/company/en/ourcompany/company_milestones.html
- PCI SSC. (2009). *Skimming prevention-Best practices for Merchants*. Payment Card Industry Security Standard Council.
- Ponemon Institute. (2012). *Payment Security Practices Survey: United States*.
- Ralph Kaiser, p. a. (2014). The Cost of Accepting Payments - Why Airlines Need a Payment Strategy. UATP.
- Romney, M. a. (2012). *Accounting Information Systems 12th Edition*. Pearson.
- Sheridon, K. J. (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime*.
- Stanley, P. B. (2002). Fraud management in the credit card Industry.
- Sullivan, R. J. (2010). The changing nature of U.S. Card payment frauds. Industry and Public Policy Options. *Economic Review: The Federal Reserve Bank of Kansas City*, 101.
- Sylvester, O. (2002). *Types of credit card fraud*. Retrieved January 2015, from Transnational Credit Card Frauds: <http://people.exeter.ac.uk/watupman/undergrad/owsylves/page3.html>
- Tej Paul Bhatla, V. P. (2003). Understanding credit card frauds.
- Tesfaye, A. (2012). *Information Assimilation*. New York: xxx.
- Transnational Credit Card Frauds*. (n.d.). Retrieved from Transnational Credit Card Frauds.
- UATP. (2011). *UATP-About Us*. Retrieved January 2015, from <http://www.uatp.com/about-us/index.html>
- Visa. (2008). *Card acceptance and chargeback management guideline for Visa Merchants*. Visa Inc.

- Visa. (2014). *Card acceptance and chargeback management guidelines for Visa Merchants*. Visa Inc.
- Visa. (2014). *Chargeback management guideline*. Visa Inc.
- Visa. (2014). *Chargeback management guidelines for Visa Merchants*. Visa Inc.
- Visa Europe. (2014). Managing payment card fraud - a guide for airlines.
- WorldPress. (2014, May). *Cashless Society*. Retrieved March 2015, from <https://wireless.kth.se/cashlessociety/>
- Yin, R. K. (2011). *Qualitative Research from Start to Finish*. New York: The Guilford Press.
- Yin, R. K. (2011). *Qualitative Research from Start to Finish*. New York: The Guilford Press.
- Yogi, H. (2011). Building our defence against credit card fraud: a strategic view. *Journal of Money Laundering Control*, 2.

7. Annexes

7.1. Annex I: Questionnaire

Addis Ababa University
School of Business and Public Administration
Department of Accounting and Finance

Dear Respondent,

In partial fulfilment of the requirements for the Degree of Master of Science in Accounting & Finance at Addis Ababa University, I am undertaking a research on The “***Current Practices and Challenges of Using Credit Card as a Payment Method: The Case of Ethiopian Airlines***”. I have therefore, prepared this survey questionnaire with a view to gathering relevant data to further understand, analyze and come up with better recommendation.

The major objective of the study is therefore, to explore the strengths and weaknesses of Ethiopian Airlines’ credit card sales management systems in handling chargebacks and managing credit card frauds. This questionnaire is also believed to produce very valuable inputs to the improvement of the credit card sales management system of the airline.

This questionnaire contains 4 parts and may take a maximum of 25 minutes to complete. Therefore, your cooperation in filling out the questionnaire honestly, carefully and timely is extremely valuable.

Finally, I want to kindly assure you that the items included in this questionnaire are not designed to test your ability or level of understanding and that all the information you provide will exclusively be used for the purpose of academic research only and will be kept in strict confidentiality.

Thank you for your kind cooperation in advance!

Temesgen Getaye

Part I: Background information

Instruction: Please put (√) sign on the box of your choice

1. Name (Optional) _____
2. Your gender?
☐ Female
☐ Male
3. Your level of education:
☐ Diploma
☐ Bachelor degree
☐ Masters Degree
☐ Other (specify) _____
4. Which of the following best represents your current position?
☐ Ethiopian Airlines sales agent
☐ Travel agent
☐ Airport or station manager of Ethiopian Airlines
☐ Area Manager of Ethiopian Airlines
☐ E-Commerce staff of Ethiopian Airlines
☐ IT Commercial support of Ethiopian Airlines
☐ Credit Analyst or Manager or Director at Finance Department of Ethiopian Airlines
☐ Payment Consolidator
☐ Customer
5. For how many years have you worked in this role and with EAL, if you are in one of the first 8 above OR for how long you use EAL in case you are customer?
☐ 1-5 years
☐ 6-10 years
☐ 11-15 years
☐ Over 15 years

Instruction: Part 2 to Part 3 of this questionnaire includes lists of statements to be answered based on Likert scale.

Please draw a circle on the appropriate response to each question using the following Likert scale:

- 1 = Strongly Disagree
- 2 = Disagree
- 3 = Undecided/Don't know
- 4 = Agree
- 5 = Strongly Agree

A. Operational Theme

2.1 In a face-to-face (Card Present) environment	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1. Universal Credit Card Charge Form (UCCCF) is completed by the customer or card holder without fail.	1	2	3	4	5
2. The agent always requests the customer to sign the form (UCCCF).	1	2	3	4	5
3. The agent maintains a copy of this form in a safe location that meets the Payment Card Industry (PCI) data security standards.	1	2	3	4	5
4. Validity and expiry date of credit cards have been regularly checked by the selling agent before accepting credit card sales.	1	2	3	4	5
5. Travel agents and/or selling agents always request authentication of the cardholder's identity and authorization of transactions by issuing banks and make sure that the transaction is legitimate.	1	2	3	4	5
6. Selling agents always obtain a valid approval code from the issuing bank or card scheme for the transaction amount before accepting credit card payment and issuing ticket.	1	2	3	4	5

7. Sales agents generally recognize that receipt of an approval code from the issuing bank does not guarantee the transaction.	1	2	3	4	5
8. If the issuing bank declines to approve the transaction the sales agent returns the card and instruct the cardholder to call the card issuer for more information.	1	2	3	4	5
9. If the issuing bank requests further information before issuing approval code, the sales agent asks the cardholder to speak directly with the issuing bank.	1	2	3	4	5
10. The sales agent requests the cardholder for passport or national identification card and verifies the cardholder's signature against that of the credit card.	1	2	3	4	5
11. The agent compares the name and account number on the card to those on the transaction receipt.	1	2	3	4	5
12. For magnetic-stripe card transactions, the agent always matches the name and last four digits of the account number on the card to those printed on the receipt.	1	2	3	4	5
13. When a signature has been obtained, the agent always matches the signature on the back of the card to the signature on the receipt.	1	2	3	4	5
14. For suspicious or non-matching signatures, the agent always declines to accept the credit card and asks the cardholder to bring an alternative payment method.	1	2	3	4	5
15. The selling agent always uses common sense and appropriate caution when evaluating any customer behaviour or other irregular situation that may occur during a transaction.	1	2	3	4	5
16. Sales agents use key - entered transactions	1	2	3	4	5

only on exceptional cases and use POS machines or magnetic stripes to swipe credit cards in most cases.

17. The selling agent always capture the card details (card number, cardholder name, expiry date, and where applicable, effective date of the card) by use of a card imprinter, or electronic card reader or card swipe.

1

2

3

4

5

2.2 Card-not present (non-face-to-face) environment and general questions	Strongly				Strongly
	Disagree	Disagree	Neutral	Agree	Agree
1. The sales agent always includes an Address Verification Service request with the transaction authorization request to the issuing bank.	1	2	3	4	5
2. For card not present transactions the sales agent always requests the cardholder for three letter codes or card verification code(CVX2).	1	2	3	4	5
3. The sales agent therefore, sends the CVX2 code to the issuing bank as part of a request for authorization of the CNP transaction .	1	2	3	4	5
4. My immediate supervisor knows the volume of charge back we receive every day.	1	2	3	4	5
5. My immediate supervisor reminds me to follow procedure to avoid charge back losses.	1	2	3	4	5
6. There is adequate and recurrent training for operational and back office staffs about credit card security and fraud prevention.	1	2	3	4	5
7. My immediate supervisor regularly discusses with me about the fraud rate and possible solutions.	1	2	3	4	5
8. I fully understand what is expected from myself to protect the sells from any chargeback	1	2	3	4	5
9. I know what PCIDSS standard is and my immediate supervisor also ensures compliance to this standards.	1	2	3	4	5
10. Sales agents know that they are the first person to mitigate or avoid chargebacks and assist the merchant to reduce revenue losses.	1	2	3	4	5

11. Sales agents and others involving in chargeback handling know that chargeback notices from the acquirer bank shall be disputed/responded in a short period of time usually in 10 to 15 days.	1	2	3	4	5
12. Sales agents and others involving in chargeback handling know that if no reponse is given to the acquirer within the disputed period the airline will lose the sales and also pays associated chargeback processing costs.	1	2	3	4	5
13. Chargeback notices from the acquirer bank is always forwarded to the right station or area offices or sales agent in a timely manner from ET's Treasury office.	1	2	3	4	5
14. Ering stations or sales agents always respond to Finance office/Treasury with as much information and supporting documents as possible to the acquirer to help them remedy the chargeback within the disputed period.	1	2	3	4	5
15. When cardholders contact ET offices directly with claims or with a dispute, the office addresses all of the cardholder's pertinent claims and issues the refund or resolve the dispute on a timely basis.	1	2	3	4	5

B. Technical & Administrative Theme

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1. Credit Card Fraud is one of the biggest threats to business establishments today.	1	2	3	4	5
2. Ethiopian is far more at risk from credit card fraud than the cardholders.	1	2	3	4	5

3. Fraudulent charges caused Ethiopian lose the cost of the product or services sold, pay chargeback fees, and fear from the risk of having their merchant account closed.	1	2	3	4	5
4. EAL has fraud screening tools to secure all of its selling channels.	1	2	3	4	5
5. Fraud prevention procedures used by EAL is good enough to make a secure card business.	1	2	3	4	5
6. The financial risk of credit card sales is effectively monitored within EAL.	1	2	3	4	5
7. EAL has a well-organized credit card office that navigates the business environment and update operational stuffs about how to make a secured business.	1	2	3	4	5
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
8. EAL has efficient system to transmit fraud alerts across divisions and take immediate action.	1	2	3	4	5
9. EAL has a knowledge sharing system about fraud detection and prevention best practices.	1	2	3	4	5
10. Ethiopian airlines fraud risk is higher than that of the industry average.	1	2	3	4	5
11. EAL uses Velocity Checking to screen fraudulent transactions.	1	2	3	4	5
12. EAL uses Geo-location Checks to screen fraudulent transactions.	1	2	3	4	5
13. The current fraud screening tools deployed by EAL are not strong enough to protect EAL's credit card frauds.	1	2	3	4	5
14. Internal control of EAL towards credit card	1	2	3	4	5

transactions is strong.					
15. EAL makes fraud risk analysis for internal and management consumption.	1	2	3	4	5
16. Chargeback loss is insignificant for Ethiopian airline and could not be an issue.	1	2	3	4	5
17. EAL has a clear and effective management policy towards credit card fraud management.	1	2	3	4	5
18. The management policy of EAL clearly defines the roll of each division on credit card sales handling.	1	2	3	4	5
19. EAL management knows the true cost of fraudulent transactions.	1	2	3	4	5
20. Ethiopian airlines policy on fraud detection is updated every time to effectively mitigate chargeback and card frauds.	1	2	3	4	5
21. There are efficient and user friendly systems which enable Ethiopian airlines management to periodically monitor the volume of credit card sales and chargeback rates.	1	2	3	4	5

Short answer and Open-Ended Questions

1. Which of the following is used by selling agents in selling tickets through credit cards? (please tick (√) one or more as applicable)

- ☐ More of Key entry
- ☐ More of Point of Sales (POS) Machines
- ☐ More of Magnetic-stripe
- ☐ Use all the three when needed

2. Which of the following system(s) is/ are used during card acceptance process?

- ☐ AVS (Address Verification Code)
- ☐ Negative Databases
- ☐ CVX2 (Card verification code)
- ☐ Verified by Visa
- ☐ Velocity Checking
- ☐ Fraud Detection Tool
- ☐ Geo-location Checks

3. Overall, how do you rate the quality of Ethiopian airlines credit card sells management system?

4. What do you think the management of EAL should do with respect to current fraud rate

7.2. Annex II: Interview

Addis Ababa University
School of Business and Public Administration
Department of Accounting and Finance

Dear Interviewee,

The intent of this interview is to explore information regarding the current practices, challenges, and prospects of using credit cards as a payment method by Ethiopian Airlines to have sufficient understanding to the research problem in addition to questionnaires distributed to selected sales agents at area offices and around Addis Ababa and the support team at head quarter of the airline. This interview will be made with 6 purposely selected directors, managers and officers who are working as support to the operating team.

Finally, I want to kindly assure you that all the information you provide will exclusively be used for the purpose of academic research only and will be kept in strict confidentiality.

Thank you for your kind cooperation in advance!

Temesgen Getaye

Interview Questions

Here below are some general open ended questions on the current practices, challenges, and prospects of using credit cards as a payment method by Ethiopian Airlines.

1. How do you rate Ethiopian Airlines fraud prevention and fraud management practices?
2. Do you think that Ethiopian Airlines Credit Card Reconciliation and E-Commerce departments are well organized to regularly monitor the card payment industry trends, to timely handle chargebacks, analyze the airlines' fraud losses?
3. What fraud screening tools are available in the market for airlines today to detect and prevent card frauds?
4. How effective or robust are the airlines' management information systems to provide accurate, timely and complete information to management?
5. Do you believe that the airline has adequate recurrent trainings to operating and back office staff of the airline on card acceptance and fraud prevention?
6. Do you think that management is aware of the volume of chargebacks and fraudulent transactions and provide adequate support in terms of resources such as qualified staff and fraud prevention and detecting tools and technologies?
7. Do you think that the airlines' senior management give due attention to chargebacks and revenue losses due to card frauds?
8. How do you see the fraud prevention policies and procedures of the airline?
9. Do you think that roles and responsibilities of different departments of the airline relating to credit card activities have been clearly defined and separated?
10. What do you recommend for the improvement of the current fraud detection and fraud management systems and the overall internal control system on credit card acceptance and fraud management?

7.3. Annex III: Questionnaire results

ET's management know the true cost of card fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	2.1	2.2	2.2
	Disagree	25	53.2	54.3	56.5
	Neutral or don't know	7	14.9	15.2	71.7
	Agree	9	19.1	19.6	91.3
	Strongly agree	4	8.5	8.7	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Gender of respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	23	48.9	48.9	48.9
	Male	24	51.1	51.1	100.0
	Total	47	100.0	100.0	

Education level of respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Diploma	8	17.0	17.4	17.4
	Bachelor	30	63.8	65.2	82.6
	Masters	7	14.9	15.2	97.8
	Other	1	2.1	2.2	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Current position of respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ET Sales agent	17	36.2	37.0	37.0
	Travel Agent	1	2.1	2.2	39.1
	Airport or station manager	1	2.1	2.2	41.3
	Area manager	14	29.8	30.4	71.7
	E-Commerce staff	2	4.3	4.3	76.1
	Finance staff	10	21.3	21.7	97.8
	Payment consolidator	1	2.1	2.2	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Year of service in current position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-5 years	16	34.0	34.8	34.8
	6-10 years	7	14.9	15.2	50.0
	11-15 years	9	19.1	19.6	69.6
	Over 15 years	14	29.8	30.4	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Completion of UCCCF by customer

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	2	4.3	4.4	4.4
	Disagree	6	12.8	13.3	17.8
	Neutral or don't know	11	23.4	24.4	42.2
	Agree	17	36.2	37.8	80.0
	Strongly disagree	9	19.1	20.0	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

Operating staff maintain cc records safely per CPIDSS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	9	19.1	19.6	19.6
	Neutral or don't know	20	42.6	43.5	63.0
	Agree	9	19.1	19.6	82.6
	Strongly agree	8	17.0	17.4	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Request the issuing bank for authentication of the card

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	8	17.0	17.4	17.4
	Neutral or don't know	12	25.5	26.1	43.5
	Agree	17	36.2	37.0	80.4
	Strongly agree	9	19.1	19.6	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Obtain valid approval code from the issuing bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	2.1	2.3	2.3
	Disagree	5	10.6	11.4	13.6
	Neutral or don't know	11	23.4	25.0	38.6
	Agree	19	40.4	43.2	81.8
	Strongly agree	8	17.0	18.2	100.0
	Total	44	93.6	100.0	
Missing	System	3	6.4		
Total		47	100.0		

Awareness that receipt of an approval code does not guarantee payment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	3	6.4	6.7	6.7
	Disagree	18	38.3	40.0	46.7
	Neutral or don't know	11	23.4	24.4	71.1
	Agree	10	21.3	22.2	93.3
	Strongly agree	3	6.4	6.7	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

Agents requests customer to show passport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	11	23.4	23.9	23.9
	Neutral or don't know	6	12.8	13.0	37.0
	Agree	16	34.0	34.8	71.7
	Strongly agree	13	27.7	28.3	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Agents use less key entry

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	11	23.4	24.4	24.4
	Disagree	13	27.7	28.9	53.3
	Neutral or don't know	11	23.4	24.4	77.8
	Agree	8	17.0	17.8	95.6
	Strongly agree	2	4.3	4.4	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

Agents include AVS in the authentication request

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	10	21.3	22.2	22.2
	Neutral or don't know	13	27.7	28.9	51.1
	Agree	18	38.3	40.0	91.1
	Strongly agree	4	8.5	8.9	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

Agents request customers to provide CVX2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	4	8.5	9.1	9.1
	Disagree	15	31.9	34.1	43.2
	Neutral or don't know	13	27.7	29.5	72.7
	Agree	11	23.4	25.0	97.7
	Strongly agree	1	2.1	2.3	100.0
	Total	44	93.6	100.0	
Missing	System	3	6.4		
Total		47	100.0		

There is adequate recurrent training for operating and back office staff on credit card and card fraud management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	18	38.3	39.1	39.1
	Disagree	10	21.3	21.7	60.9
	Neutral or don't know	8	17.0	17.4	78.3
	Agree	8	17.0	17.4	95.7
	Strongly agree	2	4.3	4.3	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Staff are aware of what is expected of them

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	2	4.3	4.3	4.3
	Disagree	15	31.9	32.6	37.0
	Neutral or don't know	7	14.9	15.2	52.2
	Agree	11	23.4	23.9	76.1
	Strongly agree	11	23.4	23.9	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Operating staff knows about PCISS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	2.1	2.2	2.2
	Disagree	14	29.8	31.1	33.3
	Neutral or don't know	21	44.7	46.7	80.0
	Agree	5	10.6	11.1	91.1
	Strongly agree	4	8.5	8.9	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

Sales agents know that they are the first person to protect fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	16	34.0	34.8	34.8
	Neutral or don't know	10	21.3	21.7	56.5
	Agree	11	23.4	23.9	80.4
	Strongly agree	9	19.1	19.6	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

ET's staff know about chargeback dispute priod

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	9	19.1	19.6	19.6
	Neutral or don't know	19	40.4	41.3	60.9
	Agree	9	19.1	19.6	80.4
	Strongly agree	9	19.1	19.6	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Credit card fraud becomes a major threat to businesses today

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	6	12.8	12.8	12.8
	Neutral or don't know	7	14.9	14.9	27.7
	Agree	14	29.8	29.8	57.4
	Strongly agree	20	42.6	42.6	100.0
	Total	47	100.0	100.0	

ET is far at risk than the industry average

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	8	17.0	17.0	17.0
	Neutral or don't know	8	17.0	17.0	34.0
	Agree	17	36.2	36.2	70.2
	Strongly agree	14	29.8	29.8	100.0
	Total	47	100.0	100.0	

ET has fraud screening tools to all of its sales channels

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Strongly disagree	3	6.4	6.4	6.4
Disagree	18	38.3	38.3	44.7
Neutral or don't know	13	27.7	27.7	72.3
Agree	10	21.3	21.3	93.6
Strongly agree	3	6.4	6.4	100.0
Total	47	100.0	100.0	

ET has effective fraud prevention procedures

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Strongly disagree	7	14.9	14.9	14.9
Disagree	23	48.9	48.9	63.8
Neutral or don't know	10	21.3	21.3	85.1
Agree	6	12.8	12.8	97.9
Strongly agree	1	2.1	2.1	100.0
Total	47	100.0	100.0	

ET regularly monitors the financial risks due to card fraud

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Stringliy disagree	5	10.6	10.6	10.6
Disagree	18	38.3	38.3	48.9
Neutral or don't know	14	29.8	29.8	78.7
Agree	7	14.9	14.9	93.6
Strongly agree	3	6.4	6.4	100.0
Total	47	100.0	100.0	

ET has a well-organized credit card office

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	11	23.4	23.9	23.9
	Disagree	16	34.0	34.8	58.7
	Neutral or don't know	12	25.5	26.1	84.8
	Agree	4	8.5	8.7	93.5
	Strongly agree	3	6.4	6.5	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

ET has a knowledge sharing system to educate its staff

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	4	8.5	8.7	8.7
	Disagree	27	57.4	58.7	67.4
	Neutral or don't know	10	21.3	21.7	89.1
	Agree	5	10.6	10.9	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

ET uses velocity checking

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	2.1	2.2	2.2
	Disagree	12	25.5	26.7	28.9
	Neutral or don't know	29	61.7	64.4	93.3
	Agree	3	6.4	6.7	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

ET uses geo-location system

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	2.1	2.2	2.2
	Disagree	10	21.3	22.2	24.4
	Neutral or don't know	25	53.2	55.6	80.0
	Agree	8	17.0	17.8	97.8
	Strongly agree	1	2.1	2.2	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

ET has no strong fraud screening tools to all its sales channels

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	2.1	2.1	2.1
	Disagree	12	25.5	25.5	27.7
	Neutral or don't know	9	19.1	19.1	46.8
	Agree	20	42.6	42.6	89.4
	Strongly agree	5	10.6	10.6	100.0
	Total	47	100.0	100.0	

ET's internal control to mitigate card fraud risk is strong

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	4	8.5	8.7	8.7
	Disagree	21	44.7	45.7	54.3
	Neutral or don't know	9	19.1	19.6	73.9
	Agree	10	21.3	21.7	95.7
	Strongly agree	2	4.3	4.3	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

ET has clear and effective management policy to mitigate card fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	3	6.4	6.7	6.7
	Disagree	22	46.8	48.9	55.6
	Neutral or don't know	10	21.3	22.2	77.8
	Agree	8	17.0	17.8	95.6
	Strongly agree	2	4.3	4.4	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

Roles are clearly defined by policy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	2.1	2.2	2.2
	Disagree	22	46.8	48.9	51.1
	Neutral or don't know	13	27.7	28.9	80.0
	Agree	6	12.8	13.3	93.3
	Strongly agree	3	6.4	6.7	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

ET's policy on credit card acceptance is regularly updated

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	2	4.3	4.4	4.4
	Disaagree	23	48.9	51.1	55.6
	Neutral or don't know	13	27.7	28.9	84.4
	Agree	5	10.6	11.1	95.6
	Strongly agree	2	4.3	4.4	100.0
	Total	45	95.7	100.0	
Missing	System	2	4.3		
Total		47	100.0		

There are efficient and user friendly information system

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	12	25.5	26.1	26.1
	Disagree	13	27.7	28.3	54.3
	Neutral or don't know	13	27.7	28.3	82.6
	Agree	5	10.6	10.9	93.5
	Strongly agree	3	6.4	6.5	100.0
	Total	46	97.9	100.0	
Missing	System	1	2.1		
Total		47	100.0		

Which method is used for credit card data entry for authentication

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	More of key entry	35	74.5	85.4	85.4
	More of POS	2	4.3	4.9	90.2
	More of magnetic stripe	2	4.3	4.9	95.1
	Any two or more of above	2	4.3	4.9	100.0
	Total	41	87.2	100.0	
Missing	System	6	12.8		
Total		47	100.0		

Which card fraud screening tools are in use by ET

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	AVS	16	34.0	42.1	42.1
	Negative database	2	4.3	5.3	47.4
	CVX2	4	8.5	10.5	57.9
	VbV	2	4.3	5.3	63.2
	Fraud detection tools	1	2.1	2.6	65.8
	Any two or more of the above	13	27.7	34.2	100.0
	Total	38	80.9	100.0	
Missing	System	9	19.1		
Total		47	100.0		

Overall ET's internal control system rating

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very weak	10	21.3	27.0	27.0
	Weak	15	31.9	40.5	67.6
	Average	4	8.5	10.8	78.4
	Good	6	12.8	16.2	94.6
	Very good	2	4.3	5.4	100.0
	Total	37	78.7	100.0	
Missing	System	10	21.3		
Total		47	100.0		

Overall ET's internal control system rating

