



Challenge and prospect of credit card sales management system: Case study in Ethiopian airlines enterprise

By: Abraham Zerihun Hassen

Advisor: Alem Hagos (phd)

**St Mary's university
School of Business and Economics
Department of Accounting and Finance**

June, 2015

Contents

Chapter One	4
Back ground of the study	4
1.2 Statement of the problem	4
1.3 Research questions.....	5
1.4.2 Secondary objective.....	6
1.5 Significance of the research.....	6
1.6.2 Scope of the study.....	6
CHAPTER TWO	8
LITERATURE REVIEW	8
Introduction.....	8
2.1 Meaning and Definition of Credit card.....	9
2.2 The payment industry and chargeback risks	9
2.2.1 Why Charge back.....	10
2.2.2 Credit card sales and Charge backs management	11
2.3 Credit card Hacking	13
2.3.1 Card security and battling fraud.....	14
2.3.1 Card skimming.....	15
2.4 Standard credit acceptance procedure in the airline industry	16
2.4.1 Best card acceptance procedure	16
2.5 Fraud Prevention standards of the payment industry	17
2.5.1 Know your customer.....	17
2.5.2 Fraud Screening	19
2.6 Payment industry standards across sales channel	19
2.6.1 Fraud risk in card present environment	20
2.6.2 Fraud risk in card not present environment	22
2.7 Payment card industry PCI/DSS	23
2.8 Corporate policies and internal control on fraud prevention	25
2.8.1 Corporate policy towards fraud	26
2.8.2 Division of roles and responsibilities.....	28
2.8.2.1 Objectives of organization with respect to fraud	28
2.8.2.2 Human resources disciplinary procedures	29
2.8.3 Preservation of evidence	31
2.9 Payment industry in Ethiopia.....	31

Credit card management system: special emphasis on Ethiopian airlines

2.9.1 Credit card in Ethiopia	32
CHAPTER THREE	33
RESEARCH METHODOLOGY	33
3.1 Research Design	33
3.2 Setting and strategy.....	33
3.3 Target Population and Sampling Frame	34
3.3.1 Target Population.....	34
3.3.2 Sampling Frame.....	34
3.4 Instruments of Data Collection	35
3.4.1 Data analysis and procedure	35
Instrument	35
3.5 Data Organization and Analysis	36
CHAPTER FOUR.....	37
DATA PRESENTATION AND ANALYSIS	37
4.1 Characteristics of Respondents	37
4.2 Structure, policy and standard compliance towards credit card sales (Organizational theme)	37
4.2.1 Compliance to international standards and internal corporate policy	38
4.2.2 Ethiopian airlines credit card management system efficiency	39
4.3 Ethiopian airlines Credit card sales (Operational theme).....	40
4.3.1 Ethiopian airlines card acceptance procedure and the scheme rule	40
4.3.2 Fraud screening in Ethiopian airlines.....	40
4.4 Technical and system issues towards credit card acceptance and charge back management.....	41
4.4.1 Fraud rate and sales volume.....	41
4.4.2 Fraud rate in card present and card not present transactions.....	43
4.4.3 Charge back response time.....	44
4.4.4 Fraud rate across region	45
CHAPTER FIVE	47
FINDINGS, CONCLUSION AND RECOMMENDATION	47
5.1 Summary of Findings	47
5.2 Conclusion	48
5.3 Recommendation	48
Bibliography	50
Annex II Personal consumption expenditure prediction by Nelson	58
Annex III High fraud count by regions	59

Chapter One

Back ground of the study

Operating in the cash less environment is the most suitable medium of making business. Backed by the technology advancement the future economy will definitely avoid the paper money from the business cycle. Specially the modern economy drove off the paper money transaction from the economy; almost all economies of the world promote cash less society as it has its own significance in terms saving and financial management

Though credit transacting has abundant gains but it is also risky and requires technology and working together across a number of companies. Most companies who uses credit cards and other alternative forms of payment suffer from credit risk as some of the money went uncollectable.

This study focuses on the challenges of credit card management system and the credit risk mitigation practices of Ethiopian airlines enterprise. Ethiopian Airlines works almost in 6 continents of the world and the nature and the financial structure of each market shaped the sales structure and the financial treatment of the sales in the way that can entertain various forms of payment

1.2 Statement of the problem

Availing multiple payment option becomes mandatory to survive the market competition, specially in international business like airline industry which shows higher volatility on customers choice. To achieve this goal (increasing the market share) most airlines provide a number of brand new payment options which are attached to financial risks. An article released in 2013 by LexisNexis explain the cost of fraud in reference to merchants cost of \$2.79 for each dollar of fraud losses they incur, up by \$0.10 on the dollar from 2012 (LexisNexis, 2013)

Usually charge back loss originates from any system or manual error at the point of card acceptance which will subsequently cause revenue degradation. Merchants always search for fraud protection way to know how can they effectively battle charge back, the contribution of internal control system to fraud reduction need to measured loop wholes on credit card sales management need to be searched and listed

Ethiopian airlines promote working in the cash less markets, where the fraud risk causes lots of damage to companies revenue. So this study focused on the level of fraud risk in EAL in terms of the company's sales volume, available seat and partner's trust and measures its relation with the existing internal control structure. Further this study evaluates the accounting treatments, assess the business process /flow and propose feasible measures

Adherence to PCIDSS standard (payment card industry & Data security standard) ensures secured credit card transaction. These standards argue every card number is precious property

of the card owner which needs to be saved in encrypted format and ensure no operational staff has access to card detail. Accordingly Ethiopian compliance to this standard needs to be measured.

It is important to note that fraud and charge back are not the problem of western economies rather a huge fraud report is witnessed in African countries like Nigeria, South Africa and Kenya. In Dec2014 The Guardian reported detention of 77 hackers in Kenya alone (Guardian, 2014) , Ethiopian airlines flew to all of these countries and avail credit card as one form of payment option. This confirm that the company's exposed to fraud on this markets need to searched and analyzed

Every card holder is a customer for the card issuing bank and for the merchant (like airlines) so that any mischief made on the card will affect both the merchant and the card issuing bank. With the interest of protecting their customer card schemes (like VISA co. and Master Co.) follow up fraud count caused by merchants' poor control system. Accordingly excessive fraud count on the merchant may lead to progressive penalty levied by the schemes or in the worst case scenario it may even lead to revocation of card acceptance. In light of this reality the whereabouts of EAL's fraud level need to be checked on top priority before it cause eminent penalty and revocation by the schemes.

1.3 Research questions

This study assesses the current practice of Ethiopian airlines credit card handling system and answer the following main research questions

- Is there any deviation on Ethiopian airlines card acceptance process when compared to the standards given by the schemes?
- How serious is the fraud risk in Ethiopian airlines?
- Does Ethiopian airlines have competent fraud screening system
- How qualified and competent are the selling agents in terms of verifying card and detecting counterfeit on card acceptance
- What are the weaknesses in charge back management practices of the airline?
- Are there suitable control mechanisms for avoiding charge backs/ credit risk?
- What feasible administrative actions can Ethiopian airlines place to mitigate the fraud risk
- Is there performance auditing practice to evaluate the effectiveness and efficiency of Ethiopian credit card handling system

1.4 Objectives of the research

1.4.1 Primary objectives

The primary objective of this research is to assess the airline's strength and weakness towards credit card sales management system and measure any deviation from the industry standard. It also measures the company's adherence to the international guidelines and forward possible solutions to battle charge back losses

1.4.2 Secondary objective

The secondary objective of this research is to evaluate the business process flow, accounting treatment and standards used by Ethiopian airline in handling credit card transactions and to find out the major reason that cause un-collectability expense to the airline

1.5 Significance of the research

Doing business thru credit card transaction will directly bring the fraudsters to the merchants online place of business, Associated Press release shows that hacker gang that looted as much as \$1 billion worldwide only in 2013 (Associated Press (AP), 2015)

In line with the fraud risk of the global market, Ethiopian airlines fraud count increases from time to time which subsequently bring financial loss to the company. The significance of this study magnifies when we see the growth of credit card transaction over cash based transaction, currently 40% of Ethiopian airlines sales is made thru credit card, and technically all of this transaction might bring charge back loss. So this study analyzes the whole credit card transaction flow to identify the system and procedure gap. More over this research extend it scope to address the pain point and contribute a piece in avoiding charge back losses

The findings will enable the company to understand the loop hole in the current practice and future factors that would adversely affect the company's revenue maximization target. Apart from those, the study can serve as a reference material for other researchers who are interested to investigate such topic in more detailed manner.

1.6. Definition of terms, Scope and limitation of the study

1.6.1 Definition of terms

The following key terms are defined in the context of Ethiopian airlines and the payment industry

Merchant: a company involved in international trade, especially in E-commerce

Acquirer: is a financial institution that processes credit or debit card payments on behalf of a merchant

Sales volume: is the amount of total sales through ticket offices

Fraudulent transaction: Sales made to a card which is stolen or hacked

Charge back: re-claimed amount of sales due to fraud transactions thru stolen cards by hackers

Card Scheme: Card issuing companies like VISA Co and MASTER Co

1.6.2 Scope of the study

This research is confined to the Head Office level; this is because Ethiopian airlines generally adopt a centralized system for credit card transactions. Whilst the sample survey and interview is stretched to operation areas like ticket offices, airports and account managers from the acquiring bank

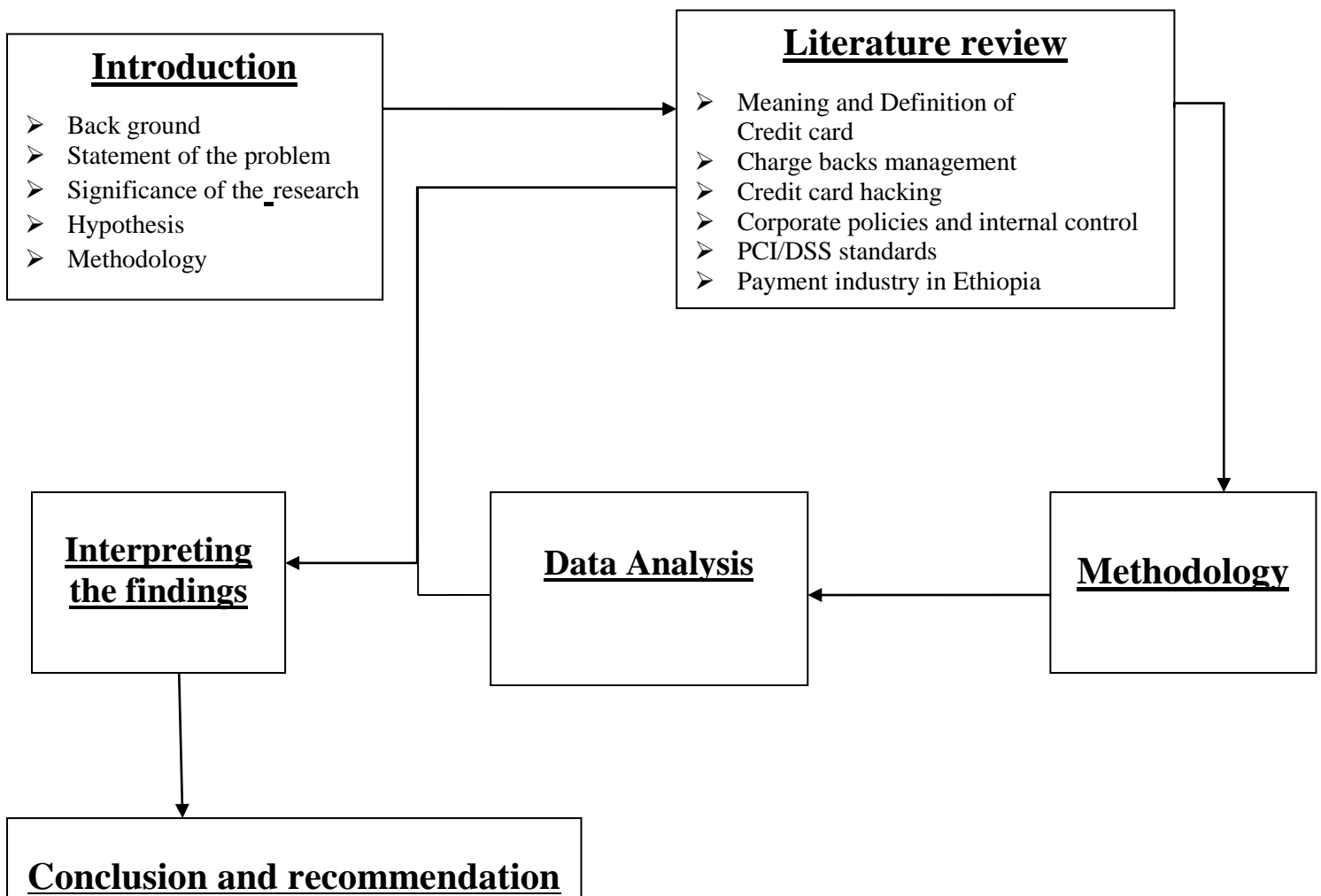
1.6.3 Limitation of the study

Due to the confidentiality of financial information, the researcher is unable to get detailed data about the fraud count and magnitude of charge back, rather the company avail the data only in percentage form. For the sake of conciseness and relevance, the researcher chooses to concentrate on practices of credit card handling for short period. In addition due to the lack of previous research work in Ethiopian context on these topic this research took foreign articles, periodicals by schemes, report of government offices and other electronic source like media news

1.7 Outline of the proposed research report

This research paper has four chapters. The first chapter present the back ground of the paper and the highlight of what the researcher wants to do. And the second chapter focuses on the literatures related to this topic; the third chapter presents the analysis part and show clearly interpret what the finding mean. Chapter four is the last chapter and it concludes and recommend based up on the findings of the analysis. The organization of the paper and the research flow is depicted on the below chart

Figure 1.1 Outline of the thesis



CHAPTER TWO

LITERATURE REVIEW

Introduction

The payment card industry consists of all the organizations which store, process and transmit cardholder data, usually for debit cards and credit cards. Number of card types circulate in the payment industry the dominant ones include Charge card, Credit card, Debit card, ATM card, Stored-value card and Fleet card, one evolved from the idea of the prior card type, the industry introduces lots of card products.

From all these card types fraud risk is dominant on credit cards though lots of rules and regulations are applied on card present and card not present transactions. A rising portion of travel sales are conducted with customers in a non face-to-face environment. Because of this, the risk of accepting credit card transactions that are later identified as fraud has increased. In an attempt to remain competitive, in a market where customers expect to purchase travel from the comfort of their home, travel agents often accept credit card payment from first-time customers with very little identifying information. By supporting this type of distribution, merchant agents take the risk that customers are committing fraud, so weigh the pros and cons. The standard requires use of magnetic stripe on a card to process transactions because its security relies on the holder's signature and visual inspection of the card to check forgery. A research made by the U.S. trade commission on July 12th, 2014 shows a worldwide fraud of \$5.55 Billion (United States Federal Trade Commission, Consumer Sentinel Network, U.S. Department of Justice, 2014)

The security standards are developed by the Payment Card Industry Security Standards Council which develops the Payment Card Industry Data Security Standards used throughout the industry. Individual card brands establish compliance requirements that are used by service providers and have their own compliance programs. Major card brands include American Express, Discover Financial Services, Japan Credit Bureau, MasterCard Worldwide and Visa International. Most companies use member banks that connect and accept transactions from the card brands. Not all card brands use member banks, like American Express, these instead act as their own bank.

Within the payment industry some sectors aligned together to work together for marketing and strategic reasons. The airline sector has joined the UATP (Universal Air Travel Plan) UATP is the airline owned payment network accepted by thousands of merchants for air, rail, hotel and travel agency payments.

In peruse of a secured and fraud free sales outlet companies specially in the developed nation are promoting alternative forms of payment than card payments. The industry introduce a brand new payment solution like Apple Pay, Google Wallet and a few other services which uses a wireless technology called near-field communication, or NFC. With Apple Pay, the phone unlocks automatically when customers hold it near the NFC reader on the merchant's payment system. These technologies provide additional layer to the merchants fraud protections system at the time of the transaction the customer is prompted to scan his fingerprint to authorize the transaction.

2.1 Meaning and Definition of Credit card

Credit cards are defined by business dictionary as “a standard-size plastic token, with a magnetic stripe that holds a machine readable code”. Credit cards are a convenient substitute for cash or check, and an essential component of electronic and internet commerce. The rising interest in e-commerce and electronic payment techniques have increased more in number, probably due to its simplicity. The card user is expected only to enter the card numbers, then the merchant get these validated and process the payment be made right away.

Many scholars and web sources argue the concept of using a card for purchases was described in 1887 by Edward Bellamy in his utopian novel Looking Backward. Bellamy used the term credit card repeatedly in this novel, although this referred to a card for spending a citizen's dividend from the government, rather than borrowing. This concept is a bit similar in functions to the current Social Security Cards (EDWARD)

A credit card holders is a person who may pay periodic service charges to use a card which enable them withdraw on limited credit approved by the card-issuer such as a bank, store, or service provider like airlines. Usually cardholders pay for credit card purchases within 30 days of purchase to avoid interest and/or penalties.

Studies made by Javelin Strategy & Research predict cards payment will grow as an online payment option at a 42% compounded annual rate, from \$6.2 billion in 2008 to \$35.5 billion in 2013. According to Javelin Credit card transactions will continue to grow online payment option, making them the fastest-growing payment method on the web and representing 13% of total online transactions in five years (Research, 2008). Furthermore, according to many experts, credit cards will continue to be the easiest option for e-commerce due to the more comprehensive online fraud protection and zero liability policies offered by major card issuers

2.2 The payment industry and chargeback risks

The payment card industry consists of all the organizations which store, process and transmit cardholder data, most notably for debit cards and credit cards. The security standards are developed by the Payment Card Industry Security Standards Council which develops the

Payment Card Industry Data Security Standards used throughout the industry. Individual card brands establish compliance requirements that are used by service providers and have their own compliance programs. Major card brands include American Express, Discover Financial Services, Japan Credit Bureau, MasterCard Worldwide and Visa International. Most companies use member banks that connect and accept transactions from the card brands. Not all card brands use member banks, like American Express, these instead act as their own bank.

As of 2014, the United States uses a magnetic stripe on a card to process transactions and its security relies on the holder's signature and visual inspection of the card to check for features such as hologram. This system will be outmoded and replaced by EMV in 2015. EMV a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions. It has enhanced security features, but is still susceptible to fraud.

Detection and prevention of fraud is an extremely important form of risk management in the credit card industry. According to a bankcard profitability study from Credit Card Management, the industry loses close to one billion dollars a year from fraud. These are losses to the card issuing companies and do not include the fraudulent transactions charged back to merchants in the mail order/telephone order (MOTO) environment. The losses associated with these attacks has risen drastically across the past years, and counterfeit fraud has now been overtaken as the most costly type of card fraud by a newer method, that of Cardholder-Not-Present (CNP) fraud. From the afore-discussed it is evident that credit card frauds offer a wider and interested area for research or study

2.2.1 Why Charge back

Chargeback on credit card sales is one of the most unpopular subjects in the travel industry. As long as card owners are not involved in the transaction or if they do not receive any product or service they are guaranteed to be protected from any charge. Charge back is a means of re-claiming an already deducted fund from the card holder's account, so for all un identified charges customer raised charge back on the merchant. And the merchants (airline in this case) and travel agents engage in a process that must be managed to respond to these inquiries (chargeback).

Usually an unsigned card could be a sign of fraud which will later result charge back to the merchant. With a fake identification, it is easy to use an unsigned card and need to be cross checked for information to spotting fake government issued identification

There is no single reason behind fraud and any explanation of it needs to take account of various factors. Accordingly CIMA (Chartered Institutes of Management Accountants) point

out the below as the major reasons of fraud looking from the fraudster's perspective (CIMA, A guide to good practice, p.14, 2009)

- Motivation of potential offenders
- Conditions under which people can rationalize their prospective crimes away
- Opportunities to commit crime(s)
- Perceived suitability of targets for fraud
- Technical ability of the fraudster
- Expected and actual risk of discovery after the fraud has been carried out
- Expectations of consequences of discovery (including non-penal consequences such as job loss and family stigma, proceeds of crime confiscation, and traditional criminal sanctions)
- Actual consequences of discovery

A common model that brings together a number of these aspects is the Fraud Triangle; it was originally introduced by *Donald R. Cressey*, a former criminologist. The fraud triangle is a model for explaining the factors that cause someone to commit occupational fraud. It consists of three components which, together, lead to fraudulent behavior (Cressey, 1973)

Figure 2.1 The fraud triangle originated, Donald Cressey's



2.2.2 Credit card sales and Charge backs management

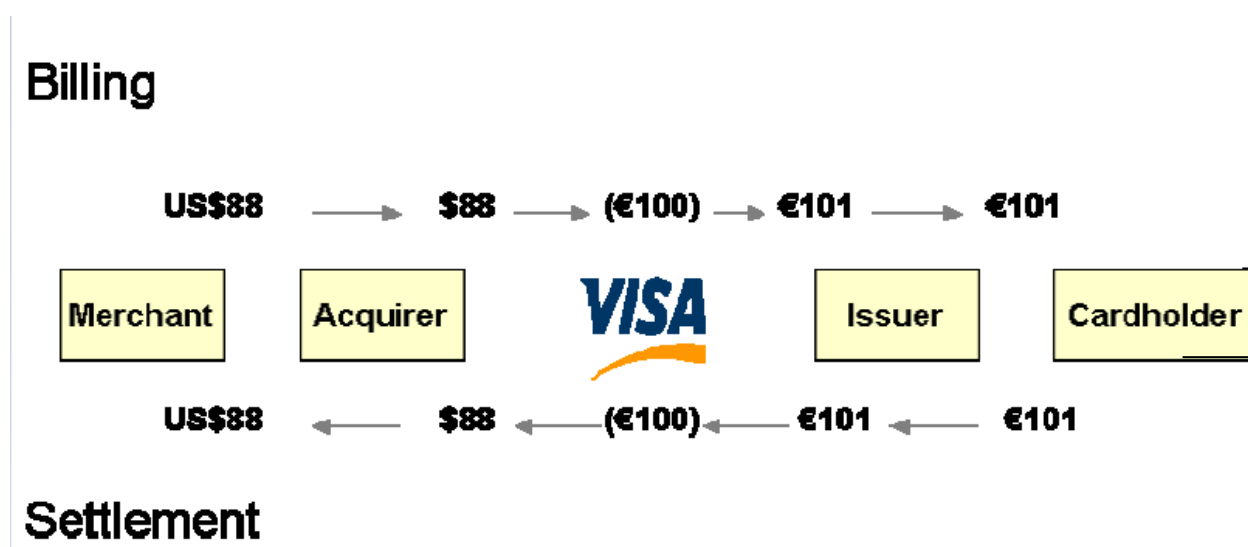
As the credit card processing became more complicated, the outer service companies started to sell processing services to clearing companies and association members. This makes to reduce the cost of programs for banks to issue credit cards and settle accounts with cardholders and this makes the greater expansion for the payments industry

Front-end processors have connections to various card associations and supply authorization and settlement services to the merchant banks'. Back-end processors accept settlements from

front-end processors. In an operation that will usually take a few seconds, the payment processor will both check the details received by forwarding them to the respective card's issuing bank or card association for verification, and also carry out a series of anti-fraud measures against the transaction.

Once the payment processor has received confirmation that the credit card details have been verified, the information will be relayed back via the system to the merchant, who will then complete the payment transaction. If verification is denied by the card association, the payment processor will relay the information to the merchant, who will then decline the transaction. The below chart can explain the whole process easily (Visa International Best Practices Guides, 2014)

Figure 2.2 - Visa multi-currency processing process Flow



A Chargeback is a reversal of a credit card transaction and usually occurs when a customer raises a dispute with their financial institution usually known as card Issuer. A chargeback may cause the amount of the original sale and a chargeback fee to be deducted from the merchant's account.

The reasons why charge backs arise vary greatly but are generally the result of a customer being dissatisfied with their purchase usually if the card holder does not get the good or the service. Fraudulent transactions thru stolen card number will also result in charge back.

Card schemes and most anti-fraud institutions agree the below are the common chargeback reasons:

- ✚ Transaction not recognized by the cardholder
- ✚ Transaction not authorized by the cardholder
- ✚ Duplicated transactions
- ✚ Cancelled recurring/direct debit transactions
- ✚ Goods/Services not received or faulty
- ✚ Goods/Services not as described

- ✚ No authorization obtained
- ✚ Fraud enquiries
- ✚ Legal proceedings
- ✚ Point-of-Sale errors

The usual chargeback process involves the below sequential flow:

1. Transaction is disputed. Cardholder raises problem with their financial institution (known as the Issuer) or the Issuer discovers a breach of the card scheme rules.
2. Issuer advises the case to the merchants acquiring bank
3. The acquiring bank request documentation from the merchant to verify the transaction. The merchant has a set timeframe to respond to retrieval requests, usually 15 days.
4. If the chargeback is invalid acquirer will decline the chargeback and return it to the Issuer.
5. If the chargeback is valid the chargeback amount is debited from the merchant's account and written notification is provided to the merchant.

A chargeback fee may also be charged to the merchants account.

2.3 Credit card Hacking

The concept of hacking as a methodology to achieve some particular goal has the allusion of working at something by experimentation or empirical means, learning about the process under review or development by ad hoc mechanisms. There is not any particular way or any life cycle to do hacking and there is no specific end goal, an improvement is in itself an achievement, but not necessarily a reason for further activity.

In the cash less environment where the vendor's shop over the internet, there are lots of ways to hack a card. The payment data transfers between the customers PC and the vendor that raises concerns about credit card online security and identity theft. Most online shops are secured to prevent unauthorized people from seeing that information and the secure site symbol should be displayed by the Web browser as proof. (FSPro Labs, 2001-2005)

There are different ways of hacking card the most common is thru successful attacking on poor web shop, it is very difficult to get the credit card details, but thousands of credit cards are compromised in a successful attack. The intellectual hackers and poor web-shop security lead to major breakings that are happening frequently. (Dara)

Phishing customers into submitting card information voluntarily is another way hackers use more frequently. Hackers created fake on-line stores that use a simulated order process designed. They use these kinds of sites only to record and to steal the credit card information. Another way is by sending fraudulent e-mail asking the person to update his registration and credit card data for a Web service to use. Many users have become victims of these credit card scams. On the positive side, fraud activity is usually detected and stopped immediately by alert Web hosts. (FSPro Labs, 2001-2005)

Hackers also attack personal computers to steal card information, most Internet Explorer users enjoy the convenient auto complete feature. It remembers data, including credit card information, used to fill in Web forms and saves it in a safety place. The next time when one is required to fill out a similar form, it completes it automatically. The problem, it is possible to capture and read the contents of Protected Storage. A fix for this credit card online security weakness was introduced that excluded credit card and other sensitive fields from auto completion. Unfortunately, a large number of online stores are not prepared to handle the fix properly, we can say this as it is not so effective in all cases. If hackers accesses ones computer directly or remotely card information can be stolen easily.

2.3.1 Card security and battling fraud

Credit card contain additional security feature called a card security code (CSC) is stamped or printed on the card; it is used as a security feature, in situations where a PIN cannot be used. A card security code (CSC), sometimes called card verification data (CVD), card verification number (CVN), card verification value (CVV or CVV2), card verification value code (CVVC), card verification code (CVC or CVC2), verification code (V-code or V code), card code verification (CCV), or signature panel code (SPC) are different terms for a security feature. This code reduce fraud incident specially in "card not present" transactions.

PIN code is not printed or embedded on the card but is manually entered by the cardholder in "card present" transactions. On the other hand there are also contactless cards which are also called chip cards; these cards electronically generate their own code.

MasterCard started issuing CSCs in 1997 and Visa in the United States issued them by 2001. American Express started to use the CSC in 1999 in response to growing internet transactions and card member complaints of spending interruptions when the security of a card has been brought into question.

Visa, MasterCard, Discover, and American Express each provide a valuable service that allows agents to validate the un-embossed code on a credit card. Validating that the un-embossed number matches the number associated with the card helps to confirm that the customer has a valid card in his/her possession. This prevents individuals with stolen credit card numbers from using the numbers to make fraudulent purchases. This tool has proven to be a valuable risk management tool. However, as with the Address Verification Service, use of this tool does not provide for a shift in liability in the event of a chargeback.

This tool is available for most card types through the system providers. Check the help screens for information about how to use CID, CVV2 and CVC2.

2.3.1 Card skimming

Skimming a card detail is the most complicated theft strategy introduced to the payment industry; skimmer copy card information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam, it is high-tech which needs credit card and banking info, hackers then print another card with the same detail which is a complete identity theft to the card owner.

A skimmer in the ATM world usually features two important pieces of hardware: A micro camera positioned within eyesight of the keypad, and a magnetic card reading device that captures your card's details. To "clone" duplicate cards, this is all the info a would-be thief needs. Then the fraudster took the money but the genuine card holder gets a call from the bank or credit card company about "strange" transactions on him/his account. (Engadget, <http://www.engadget.com/>)

Similar things happen with POS terminals in retail shops -- payment registers -- sometimes with the sales agent knowledge. Some terminals exist that will even print out a "transaction complete" record. Current reports of the modern economy name gas stations the common targeted for skimming. The below two pictures explain more how skimming works system can be installed in under two minutes and the stored card details are easily captured remotely via Bluetooth by the crook. So unless someone notices the device, or its battery dies, a thief could quickly grab hundreds of accounts from just one skimmer. (Engadget, <http://www.engadget.com/>)

Usually skimmers attach a device at the top of ATM or other machine that too cards, the attached device has a hidden micro camera to record the PIN number of the card and when a user insert the card to the machine this device will capture the card detail from the magnetic strip in less than 30 sec. The skimmer has possession of the full card detail and PIN so that they can print another card and loot as much as they want

Figure 2.3 Credit-card-skimming-explainer (Engadget, <http://www.engadget.com/>)



As shown in fig2.3 and 2.4 the part of the ATM machine was covered with external device that can read details of the card when the genuine card holder attempt to withdraw cash

Figure: 2.4 Credit-card-skimming-explainer (Engadget)



In spite of the security features introduced to the industry, skimmers come up with brand new theft techniques every time. A social experiment made (video lesson) on a link: <https://www.youtube.com/watch?v=4p6Ff7DcnBc> shows how PIN and card detail is robbed from a card holder

2.4 Standard credit acceptance procedure in the airline industry

2.4.1 Best card acceptance procedure

Most acquiring banks, card issuing companies and card regulating bodies like EMV (*Europay, MasterCard and Visa*) argue merchants adherence towards the basic fraud protecting procedures. In the air line arena carriers are recommended to comply with the below standards

Validate Acceptance of Form of Payment by Carrier

Most consumers already know where they want to go when they contact a travel agent. They usually know how they want to pay as well. When a customer presents payment, it is important to verify that the payment is valid for the selected carrier. The best way to verify this information is through IAR, the ARC Industry Agents' Handbook or through the ARC Travel Agency Communication (TAC) messages.

Disclosure of Terms and Conditions

At the time of sale, it is important to provide customers with the Terms and Conditions of the sale. This is generally completed either verbally or in writing. However in a situation where the customer is disputing something outlined in the Terms and Conditions, only a signed

Credit card management system: special emphasis on Ethiopian airlines

disclosure form acts as verification that the customer acknowledged receipt of the disclosure. In a case where the credit card is accepted via the internet, proof that the customer was required to “click to accept” is also valid acknowledgement.

The terms and condition clause should answer the below important information questions

- Can the ticket be refunded or exchanged? Are there any refund penalties?
- Can changes to the ticket be made? Are there fees?
- What are the procedures for making changes?

Credit Card Authorizations

A credit card authorization is required for every credit card transaction. The purpose of an authorization is to verify available credit and validate that the card and/or card number have not been reported lost or stolen. Credit card authorizations should be obtained through the system provider. Continue with the transaction only when an “approved” authorization response is received. If a response other than “approved” is received, request that the customer provide another form of payment. When charging a customer a Travel Agency Service Fee (TASF) a separate authorization must be obtained.

The voice authorization service should not be used as an alternative to obtain an authorization when the automated process through the system provider resulted in a “decline” (or message other than “approved”). When accepting a sale from an unknown customer, difficulty obtaining an approval code could be a sign of a problem.

Credit Card Security Features

All credit cards have security features that are designed to help identify counterfeit cards. The following are some of the features across all cards.

- Embossed card number on the front matches number located on the signature strip on the back (not including the card verification code).
 - Expiration Date
 - Magnetic stripe on the back of the card is above the signature box
- Individual credit card companies have unique security features which they usually release it on their web pages

2.5 Fraud Prevention standards of the payment industry

2.5.1 Know your customer

The best way to be protected against credit card fraud is to act in accordance with the “know your customer” principle. Whenever possible, have the customer come to the office. In a face-to-face environment, complete a Universal Credit Card Charge Form (UCCCF), obtain a valid

Credit card management system: special emphasis on Ethiopian airlines

approval code for the transaction amount, obtain an imprint of the credit card and have the customer sign the form. Maintain a copy of this form in a safe location that meets the Payment Card Industry (PCI) data security standards. It is not sufficient to have customers fax or e-mail a copy of a credit card charge form, they must be imprinted and signed in person.

In non face-to-face environment, there is always a risk of fraud so obtain as much information about the customer as possible and maintain the information for future reference. Even if the personal information does not include credit card numbers, it is equally important to keep this personal customer information secure. It is very important to know that at least one of the people traveling is also the cardholder. If they are not, the merchant is willing to risk that the cardholder will dispute the transaction

The following information can help to validate the identity of a customer and/or cardholder. It is helpful to use this information to cross reference against other available resources and to call the phone numbers to confirm that they are valid.

In addition, in the event of a credit card dispute or chargeback, the below information is very important to successfully defend the case per ARC's guideline. (Airlines Reporting Corporation(ARC), 2010)

- Passenger Name:
- Billing Street Address:
- Billing Address - City:
- Billing Address - State
- Billing Address - Zip code:
- Home Phone number:
- Work Phone number:
- Cell Phone number:
- Cardholder Name:

Address Verification Service (AVS)

The Address Verification Service allows merchant to verify that the billing address provided by the customer matches the billing address associated with the card. Address Verification has proven to be an effective tool for validating customer identity because in many instances the individual perpetrating fraud will not know the customer billing address.

Almost all guidelines from card issuing and clearing companies anticipate there will be charge back risk if the address from the credit card company does not match the address the merchant has on file (Airlines Reporting Corporation(ARC), 2010)

2.5.2 Fraud Screening

Card companies like Visa and MasterCard developed an online tool that allows merchants to authenticate the identity of a cardholder through a secret pin associated with an account. These online tools facilitate authentication by providing an interface directly to the credit card issuer so that a secret pin can be validated therefore authenticating the cardholder.

Flag checklist for acceptance of credit cards

There is risk associated with accepting any credit card transaction. Merchants' need to decide what level of risk you are comfortable with prior to issuing a ticket; ARC's guidelines assist merchant's evaluation of risk associated with a credit card transaction the below quadrant developed from ARC's guideline show what should the merchant do with respect to credit card transactions (Airlines Reporting Corporation(ARC), 2010)

Table 2.1 Fraud screening matrix

	Low Risk	Medium Risk	High Risk
Caller ID	Caller ID is local to the merchant	Caller ID identifies caller as local	Caller ID identifies caller as out of area or with no information at all
Originating airport	Originating airport is in the same region as the travel agency/merchant	Originating airport is in the same region as the travel agency/merchant	Originating airport is usually in the different region or country
Card ownership	The travel originate from the same region as the travel agent	Passenger may or may not be cardholder	Cardholder is not the passenger
Customer type	Passenger is also the card owner	Customer is new	Cardholder is not the passenger. "Customer" may use a religious title or other socially respected profession, to establish credibility
Travel type	Frequent travel/customer	Could be domestic or international travel	Highly flexible travel schedule
Date of travel	Date of departure is more than one month from date of issue	Date of departure is less than one month from date of issue	Last minute travel

2.6 Payment industry standards across sales channel

A number of techniques have been developed for displaying a diversified firm's operations as a portfolio of businesses. *Porter* explain the importance of having a diversified channel as a techniques that provide simple frameworks for charting or categorizing the different businesses in a firm's portfolio and determining the implications for resource allocation. Techniques for portfolio analysis have their greatest applicability in developing strategy at the corporate level

and in aiding in corporate review of business units, rather than in developing competitive strategy in individual industries. (Porter)

In the airline industry having multiple channels has unrepeatable role in terms of maximizing the sales volume across various nation and market structure vary from the infant payment economies to the advanced payment channels of the west. In light of this the airline industry sales channel can be broadly grouped as

2.6.1 Fraud risk in card present environment

Face to face sales:

This channel is usually called CTO/ATO sales whereby agents of an airline can charge a customer credit card and issue ticket using the ticketing system which is integrated with the card clearing company to fetch authorization whenever credit card details are inserted on the system. The selling agent is also responsible to verify the signature on the form to the signature on the credit card. If the card is not signed, request a driver's license or other form of government issued photo identification to verify the signatures.

Agency sales:

Agent sales is channel where a sales representative for an airline in a specific country or region is responsible for selling all products of the airline in its region which includes flight tickets and cargo space. A GSA will typically sell the product of more than one airline. Airlines normally use a GSA in areas that it does not operate to or from, allowing them to have sales presence in a country at lower cost than opening their own offices in short term. It may also use their services because the GSA has historical ties with travel and cargo agents which will be too time-consuming for the airline to build itself

Complete Universal Credit Card Charge Form (UCCCF)

This form should be signed and retained in the face to face transactions; obtaining a credit card authorization (completing a UCCCF form) the merchant will ensure possession of:

- Approval code of the authorization for the transaction
- Retain copy of the credit card
- The dollar amount to be billed to the credit card
- The customer's signature

Credit Card Authorization

The credit card companies do not recognize a generic credit card authorization form as a valid document to support a transaction; therefore, they are not a valid substitute for a signed, imprinted

In card present transaction the merchant should verify the genuineness of the card by checking various security features and Ensure that the card is on the selling agents hand until the transaction has been completed.

The below feature are highly recommended on card verification and can be taken as a check list to make a secured card payment (BWA Merchant service, 2012)

- Check the cardholder's signature on the receipt against the actual credit card.
- Expiration dates should be checked
- Ensure the number embossed on the front of the card matches the truncated number on the receipt.
- Does the name match the customer? For example: does the gender of the presenter match the salutation of the name printed on the card? Ask for photo identification to confirm details if suspicious.
- Does the card appear genuine? Is the embossing clear and even and does the printing look professional?

A genuine card should contain the below feature in its front and back pages

- Card Issuer's logo, may be a bank logo
 - Card number
 - Cardholder name
 - Card holder signature
 - Expiry date
 - CVV2/CVC2 – The 3 digit value located on or near the signature panel of the credit card.
 - Hologram (should appear three-dimensional and change color when tilted)
-
- Cards detail should always be swiped and never be manually entered the credit card number and extra caution should be taken if the customer requests to manually key a transaction.

Being vigilant about unusual credit card spending can help to avoid becoming a victim of a potential fraud attack. Look out for:

- Customers who appear nervous or anxious, or hurries you at closing time.
- Customers who seem to not care about the item they are purchasing. For example, those who do not check the size or the price of an item, grab several items quickly, or do not worry about the warranty.
- Customers who request immediate delivery, that is, they want to take large and expensive items immediately.
- Customers who request you to manually key the card number.
- Multiple cards presented. Be wary of people that give you more than two card numbers, or try to split the order.

Do not accept declined transactions. Note: Do not split a declined transaction into smaller amounts. If the customer does not cooperate or the details do not match, do not proceed with the transaction or ask for another form of payment.

2.6.2 Fraud risk in card not present environment

Internet sales:

As an efficient and flexible sales channel, online payment businesses are becoming an internationally success factor specially in terms of maximizing sales volume. Households ay use payment sites as a market to conduct online “garage sales”.

Call center sales (MOTO):

Call center sales is channel where a centralized office used for receiving or transmitting a large volume of requests by telephone. An inbound call center is operated by a company to administer incoming product support or information inquiries from consumers. Outbound call centers are operated for telemarketing, solicitation of charitable or political donations, debt collection and market research. A contact center is a location for centralized handling of individual communications, including letters, faxes, live support software, social media, instant message, and e-mail

Card not present transactions are those where neither the card nor the cardholder are present at the point of sale. A card not present transaction also called MOTO (Mail Order Telephone Order) is a payment transaction made where the cardholder does not or cannot physically present the card for a merchant's visual examination at the time of the sales

Merchants who accept card not present transactions face a higher risk of becoming victims of fraud as the anonymity of card not present transactions make them appealing targets for fraudsters. The following tips may help reduce the possibility of fraudulent transactions in the card not present environments.

- Obtain as much information as possible: the credit card number, name of bank, full name, address, expiry date, CVV2/CVC2 and contact telephone number (including landline). If processing the transaction via a terminal ensure you enter the card details correctly as per the operating guides for MO/TO transactions.
- Use some form of additional validations, such as the electronic white pages to cross check details provided.
- Call the customer on the quoted contact telephone number to confirm details of the order, especially for large and/or suspicious orders.
- Request further identification such as a photocopy of the front and back of the card. This will ensure the person has the card in their possession. Beware of fake photo shopping as some of our merchants have received completely bogus cards in a JPEG format. It must be a genuine photocopy.
- If you take payments via a website, contact your gateway provider and see if they have any fraud prevention software which you can utilize.
- Always obtain authorization for all card not present transactions, regardless of value, and for the full amount of the transaction. It is important to note that an authorization only confirms that funds are available at the time of the call and that the card has not been

Credit card management system: special emphasis on Ethiopian airlines

reported lost or stolen. It does not guarantee that the person quoting the card number is the owner of the card or is entitled to use the card.

- Keep all copies of correspondence including invoices, emails, quotations, faxes, proof of delivery, etc

The following Key measures are recommended as merchants should do to prevent frauds on card not present: (BWA Merchant service, 2012)

- Items ordered are an unusual quantity or multiple orders of the same item.
- Big ticket items or orders that are larger than normal for your business. If it seems “too good to be true” it probably is.
- Orders requested as urgent or for overnight delivery.
- You are not permitted to sell items that are different from the products you normally sell.
- When orders are cancelled and customer is requesting a transfer of money to a card or method other than back to the original credit card. (eg. Money order, money transfer). This is not permitted.
- Different cards are provided (including different cardholder names) but same delivery address given.
- Multiple cards presented. Be wary of people that give you more than two card numbers, try to split the order, or if one card declines and another card is readily available.
- If they do give you multiple card numbers look at the actual numbers, are the first 12 digits the same then they change the last four? For example you have been given three cards:
 - 4876 5432 1234 1145, 4876 5432 1234 5269, 4876 5432 1234 8537
- Multiple transactions charged to one card over a short period of time.
- Exercise caution when taking foreign orders. Orders from Asia, the Middle East and Africa may represent higher risk.

Remember the liability for all card not present transactions rests with the merchant. Therefore the more the information gathered to satisfy the merchant the higher the probability of making a secured credit business will be.

2.7 Payment card industry PCI/DSS

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. Any entity that comes in contact with credit card numbers is expected to be compliant with the Payment Card Industry (PCI) Security standards. The following link will provide you with the information you need to ensure that you are PCI compliant: (Airlines Reporting Corporation(ARC), 2010)

- Visa was the first to formally address the need for stronger data security policies

Credit card management system: special emphasis on Ethiopian airlines

- Visa wrote the original twelve requirements known as the Cardholder Information Security Program (CISP) which currently applies to service providers
- After CISP, credit card brands standardize requirements for cardholder information security and established the Payment Card Industry Security Standards (PCI) or in some regions the program is referred to as Account Information Security (AIS).
- PCI/ASI/CISP is *mandatory* for any entity that processes, transmits or stores cardholder data.
- Security requirements vary based on the level in which your company has been categorized.
- There are four levels and each level is primarily based on transaction volumes.

PCI (payment card industry)

One of the primary drivers of PCI with the credit card companies was to protect their brand, as merchants, to protect their brand and to convince customers that making purchases on a given website is safe. PCI associations have made it clear that fines will be assessed for failure to become compliant to the standard. The initial fine for level one merchants for failure to become compliant is \$5000, additionally, merchants can be held liable for losses associated with a hacking incident within their systems as well as one of their vendors' systems. (BWA Merchant service, 2012)

Challenging requirements for PCI

One of the new and most challenging requirements facing the airline industry is the use of encryption for all stored credit card data. The only options that would allow merchants to become compliant without encryption would be to mask or truncate the credit card numbers stored within internal systems.

Challenges of Encryption Requirements and possible solutions

The challenge with encryption is the need to be able to handle customer service issues or back office investigations that require you to see credit card numbers to resolve the following:

- Refunds
- Chargebacks
- Rejects
- Customer calls
- Investigating unmatched use
- Fraud

Merchants can take the below measures to tackle this problem with encryption

- Work with your credit card acquirer and the associations. The intent of PCI is to protect data, not to demand complete system re-writes
- Emphasize that displaying credit card information is critical to the back-end processes
- Be able to show that you have controls in place as to who can access this data and why it's necessary

Credit card management system: special emphasis on Ethiopian airlines

- Buildings with keycards and visitor sign-in stations are considered added security.

A Successful Certification as suggested by VISA

- Communication is critical to your success
- Involve your Information Security and/or Computer Security Departments
- Contact your Purchasing Department to ensure PCI language is included in new and future contracts with vendors that will have access to credit card information
- Work closely with your acquirers, they are very well versed on PCI. Point out any areas of weakness and ask for their help resolving them.

PCI Compliant and fraud

- PCI was developed to reduce hacking incidents to obtain credit card information with the intent to commit fraud.
- Perimeter Scanning done on a quarterly basis is necessary to identify any possible new weaknesses in your system that may make you more vulnerable to hacking incidents.
- When addressing fraud, Visa states, “Fraud as a percentage of Visa’s volume has decreased to an all-time low and now accounts for less than one-tenth of 1% of Visa’s global sales volume.”
- We can all agree that controls must be in place to prevent hacking, however, being compliant does not necessarily mean a reduction in fraud within the airline industry.

Fraud Deterrents Reduce Fraud

To successfully prevent fraud merchants should use all of the fraud deterrents like

- Address Verification
- CID, CVV2, CVC2 etc.
- Fraud Prompts
- Authentication Products e.g. Verified by Visa (VbV) MasterCard’s Secure Code
- Encourage the use of magnetic readers or point of sale terminals for all face to face transactions

2.8 Corporate policies and internal control on fraud prevention

Any error including agent or system error at the point of sales or accounting mischief at any point of credit card transaction will result in revenue degradation. A reliable internal control system and procedure will help to ensure a more secured transaction in which all invoices are prepared accurately and reported properly.

Merchants’ stake in the payment industry is highly increasing due to various reasons; a study conducted by Idea Works Company (A US based airline consulting organization) shows the increase of credit card revenue to \$31.5 Billion—Up Nearly 1200% since 2007. This triggered the idea of having a strong internal control system and a clearly defined company policy, which can protect the merchants’ interest ahead of the fraudsters act. (Idea Works, July 2014)

Another report released by Nelson shows that card payment continues to be the chosen payment option in US and the rest of the world. The report shows from the total 9.75trill dollar 35% uses card payments but for 2017 the card payment is expected to grow 51% of the total payment (NILSON, 2013). Annex II shows the graphic prediction of THE NILSONS report released in Dec 2013

Table 2.2 Nilson report on payment option prediction

Payment options	2007(in trill)	2007(in percentage)	2017(in trill)	2017(in percentage)
Paper	3.34	34%	2.28	16%
Card	3.38	35%	7.1	51%
Electronic	0.85	9%	1.47	11%
Non purchase	2.18	22%	3.06	22%
Total	9.75	100%	13.9	100%

2.8.1 Corporate policy towards fraud

An organization's approach to dealing with fraud should be clearly described in its fraud policy and fraud response plan. The fraud response plan is a formal means of setting down clearly the arrangements which are in place for dealing with detected or suspected cases of fraud. It is intended to provide procedures which allow for evidence gathering and collation in a manner which will facilitate informed decision-making, while ensuring that evidence gathered will be admissible in the event of any civil or criminal action.

Other benefits arising from the publication of a corporate fraud response plan are its preventive value and the likelihood that it will reduce the tendency to panic. It can help restrict damage and minimize losses, enable the organization to retain market confidence, and help to ensure the integrity of evidence. It is important that organizations have a documented plan for responding to suspected or detected cases of fraud. A fraud response plan should include a clear statement on the corporate policy with regard to dealing with fraud, and set out the roles and responsibilities of those involved in responding to suspicions. It should outline how an investigation should be handled, ensuring that due process is followed and integrity of evidence is maintained. The fraud response plan may also detail follow up action that will be taken by an organization in light of established incidents of fraud. (Visa International Best Practices Guides, 2014)

Corporate policy

The fraud response plan should reiterate the organization's commitment to high legal, ethical and moral standards in all its activities and its approach to dealing with those who fail to meet those standards. It is important that all those working in the organization are aware of the risk

of fraud and other illegal acts, such as dishonesty or damage to property. Organizations should be clear about the means of enforcing the rules or controls which the organization has in place to counter such risks and be aware of how to report any suspicions they may have. The fraud response plan is the means by which this information is relayed to all members of staff and, possibly, other stakeholders, such as customers, suppliers, and shareholders.

One question worthy of consideration is – how much publicity should be given to exposed fraud? A publicized successful fraud investigation can be a sharp reminder to those who may be tempted and a warning to those who are responsible for the management of controls. While there may be embarrassment for those who were close to the fraud and did not identify it, and an adverse impact on the organization’s public image, there can be advantages in publishing internally the outcome of a successful fraud investigation.

Regulated financial services companies do not have a choice on whether or not to keep identified cases of fraud an internal issue. These organizations are now legally obliged to report financial crime. Other businesses should follow this example and make it clear that they will not sweep fraud under the carpet. (BWA Merchant service, 2012)

Annual report

Merchant need to maintain log to produce annual report which should be submitted to the board of all investigations carried out, outcomes and lessons learned.

Enforcement policies

A growing number of organizations are introducing enforcement policies that highlight the organization’s zero tolerance approach to fraud and clearly state that if a case of fraud is identified, appropriate action will be taken and those responsible will be made an example of, no matter who the perpetrator is. For example, financial institutions are keen to demonstrate a commitment to dealing with wrongdoers and are increasingly prosecuting fraudulent employees rather than ‘sweeping the matter under the carpet’ (Visa International Best Practices Guides, 2014)

“After the transaction” Vs “Before the transaction” fraud screening strategy

Analyzing data inputs using software enables fraud examiners to analyze an organization’s business data to gain insight into how well internal controls are operating and to identify transactions that indicate fraudulent activity or the heightened risk of fraud. The user guide released by VISA(the company) classify fraud screening strategy in to “Before and After the transaction” Strategy” screening (Visa International Best Practices Guides, 2014)

On the other hand other merchants screen fraud before issuing the product or the service this one is more secured as the fraud analyst got the chance to catch the fraudster before sales this is called “Before Transaction Strategy” (Visa International Best Practices Guides, 2014)

2.8.2 Division of roles and responsibilities

CIMA (chartered institute of management accountants) argue that the division of responsibilities for fraud risk management will vary from one organization to the next, depending on the size, industry, culture and other factors. The following are some general guidelines which can be adapted to suit the individual circumstances. (CIMA(chartered institute of management accountants), January 2009)

Finance director

The finance director will often have overall responsibility for the organization's response to fraud, including the responsibility for co-coordinating any investigation and for keeping the fraud response plan up to date. They will hold the master copy of the fraud response plan, and should have their own aide-memoire to assist with the management of the investigation. The finance director will also be responsible for maintaining an investigation log. An investigations log is typically a log of all reported suspicions, including those dismissed as minor or otherwise not investigated. The log will contain details of actions taken and conclusions reached. It is an important tool for managing, reporting and evaluating lessons learned.

Managers and supervisors

Generally managers and supervisors are in a position to take responsibility for detecting fraud and other irregularities in their area. Staff must assist management by reporting any suspected irregularities. Managers and supervisors should be provided with a response card, or aide-memoire, detailing how they should respond to a reported incidence of fraud. The aide-memoire should include a list of contacts with telephone numbers.

Fraud officer (where applicable)

In larger organizations it may be appropriate to designate a senior manager as the fraud officer in place of the finance director. The fraud officer will have responsibility for initiating and overseeing all fraud investigations, for implementing the fraud response plan and for any follow-up actions. The fraud officer should be authorized to receive enquiries from staff confidentially and anonymously, and be given the authority to act and/or provide advice according to individual circumstances, and without recourse to senior management for approval. In the event that the fraud officer's superior is a suspect, he should report to a more senior manager or non executive director, perhaps the chair of the audit committee.

The fraud officer will manage any internal investigations and act as a liaison officer with all other interested parties both internal and external, including police, regulators and auditors. He should have his own job description, appropriate to the role, an extended list of contacts and his own response card. (CIMA(chartered institute of management accountants), January 2009)

2.8.2.1 Objectives of organization with respect to fraud

The organization's policy may include any or all of the following preferred outcomes in dealing with fraud.

Internal disciplinary action

It should be designed in accordance with the organization's personnel and disciplinary guidelines, so that sales and back office employee will comply to the policy. Any deviation can also be addressed thru this

A civil response

The company policy needs to be open for legal intervention whereby action is taken through the civil courts to recover losses

Criminal prosecution

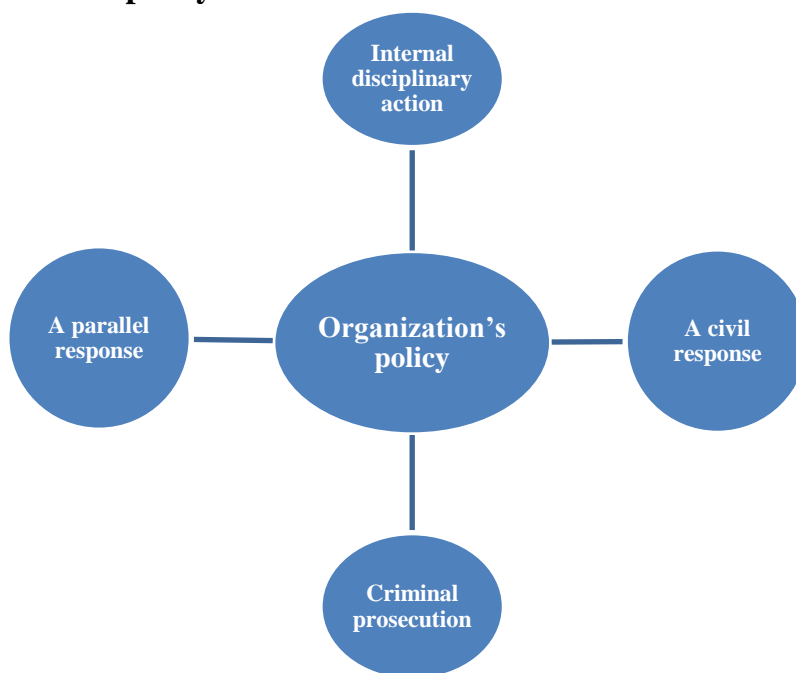
Whereby action is taken against the individual(s) concerned in a police managed enquiry.

A parallel response

Civil action need to be taken in parallel with police investigation to recover misappropriated assets

The below figure shows how these four basic themes are integrated in designing organizational policy towards fraud

Fig 2.1 Organizations policy towards fraud



2.8.2.2 Human resources disciplinary procedures

The human resources department will usually have responsibility for any internal disciplinary procedures, which must be in line with, and support, the fraud policy statement and fraud response plan. Their advice should be sought in relation to the organization's personnel management strategies, individual employment histories, and issues relating to employment law, or equal opportunities. (CIMA(chartered institute of management accountants), January 2009)

Audit committee (where applicable)

Audit committee members have responsibility for reviewing the organization's internal control and risk management systems, including the design and implementation of anti-fraud programmes and controls. The audit committee should monitor the integrity of the financial statements, assess the organization's performance in fraud prevention, review the investigation log of cases at least once a year, and report any significant matters to the board.

The audit committee should review arrangements by which employees can confidentially raise concerns about possible wrongdoing, and the audit committee's objective should be to ensure that arrangements are in place for the proportionate and independent investigation of such matters and for appropriate follow-up action. If a suspicion involves the nominated fraud contact, the finance director or an executive director, the matter should be reported directly to the chairman of the audit committee. In small companies a nominated non executive director may fulfill the role of the audit committee. The audit committee is also responsible for reviewing and evaluating the effectiveness of the internal audit function, where one exists. (CIMA(chartered institute of management accountants), January 2009)

Internal auditors (where applicable)

Where an organization has its own internal audit department the likelihood is that the task of investigating any incidence of fraud would fall to them. Caution should be exercised in allowing an investigation to be conducted by those without training and experience in this area, as this may jeopardize the outcome of an investigation. It may be appropriate to designate specific auditors as fraud specialists and to ensure that they have the appropriate skills and knowledge to undertake the task.

External auditors (where applicable)

An organization without its own internal audit department may consider consulting their external auditors should they discover a fraud, if only to obtain the expertise to establish the level of loss. The external auditors may also be in a position to provide expert assistance from elsewhere within the audit firm, such as from a specialist fraud investigation group. A decision to call on external auditors should, however, be considered carefully, as there is always the possibility that if the auditor has missed obvious fraud alerts, the organization may eventually seek damages from its auditor.

Legal advisers (internal or external)

Legal advice should be sought as soon as a fraud is reported, irrespective of the route the organization intends to follow. Specific advice would include such issues as guidance on civil, internal and criminal responses, and recovery of assets.

IS/IT staff

IS and IT staff can provide technical advice on IT security, capability and access. If computers have been utilized to commit the fraud, or if they are required for evidential purposes, specialist advice must be sought immediately.

Public relations (PR)

Organizations with a high profile, such as larger businesses, public sector organizations or charities, may wish to consider briefing their PR staff, so they can prepare a brief for the press in the event that news of a fraud becomes public.

External consultants

Any organization could consider bringing in specialist investigation skills from outside the organization. Many such specialist firms exist to provide a discreet investigation and/or asset recovery service in accordance with their clients' instructions.

Insurers

Many organizations take out fidelity insurance to protect themselves against large fraud losses. The timeframe for a report to fidelity insurers, and any additional requirements, should be included in the fraud response plan and is usually laid down in the insurance document. (CIMA(chartered institute of management accountants), January 2009)

2.8.3 Preservation of evidence

Preservation of evidence is very important to secure or preserve sufficient evidence to prove a case of fraud. It is vitally to take a due care in preserving the documents and information before it is removed or destroyed by the suspect(s). Physical evidence may therefore need to be seized at an early stage in the investigation, before any witness statements are collected or interviews conducted. In the developed nations policy will be consulted for any suspected criminal act. It is, therefore, important that proper records are kept from the outset, including accurate notes of when, where and from whom the evidence was obtained and by whom. The police, or legal advisers, will be able to advise on how this should be done. (Accelya, 2012)

2.9 Payment industry in Ethiopia

Currently most of the banks in Ethiopian issue debit cards/ATM cards, which highly facilitate the exchange of funds without paper or hard copy. This debit card are either domestic or international, the domestic card is valid only in Ethiopia which can be used specially in main cities on the other hand the international card is used to make international transactions. (National bank of Ethiopia , 2012)

The introduction of payment cards like VISA benefits the card users and banks, some of the merits are:

- Make financial transactions, including withdrawal of money without the help of a human clerk

Credit card management system: special emphasis on Ethiopian airlines

- Accessible 24 hours a day and 7 days a week
- No need to carry cash to purchase goods or services. You can transfer the sum of money needed from your account to supplier account by using POS terminal
- No need to go to the bank every time you need to withdraw money. You can access your account at any of the bank's ATM installed in various public places
- Safe from theft and lose of money
- Provides alternative services other than cash withdrawal and purchase of goods, such as mobile top up, bill payment, funds transfer, deposit, balance inquiry, etc

Lately Point of Sale Terminal (POS) is also introduced this terminal is a computerized telecommunications device that provides the customers with access to financial transactions in a public space. These POS machines enable users to

- Cash advance
- To make various payments
- To transfer funds
- Mobile top ups
- To bill payment, specially for service providing companies

2.9.1 Credit card in Ethiopia

In Ethiopia payment thru cash is the most dominant form of payment to do a business, most of the population does not have a clue about clearing payments thru card. Almost all banks issue debit cards and some issue VISA debit cards which enable payment on POS machines

The national bank of Ethiopia (NBE) allows people to use credit card as additional payment option. Accordingly anyone can use credit cards like American Express, Master, Visa, Diners Club and Cart Blanche, and Euro cards are used to authorize payments. (National bank of Ethiopia , 2012). Payment industry is at its infant stage in Ethiopia which is highly related to the growth of financial institutes like banks

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Research Design

To meet the major objectives of the research the researcher chooses to deploy both qualitative and quantitative approach in the course of data analysis. As this research focuses on the whole process efficiency and on the current challenges of credit card handling system, mixing the two approaches becomes very important. Creswell elaborate the concept of research design as 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, RESEARCH DESIGN, 2003)

Every research methodology has its own limitation so to offset the limitation one with other both qualitative and quantitative approaches are employed in descriptive manner. This type of mixed method which was applied in this research is concurrent triangulation. Triangulating data sources (a means for seeking convergence across qualitative and quantitative methods) is important (Jick, 1979 as cited in Creswell, 2007). This was because; it was helpful to the overall strength of the study than using either quantitative or qualitative research (Creswell, 2007). For this very fact, the researcher used this mixed method) to measure the effectiveness of the current practices and challenges of credit card sales management of Ethiopian Airlines

3.2 Setting and strategy

The most important condition for differentiating among the various research strategies is to identify the type of research questions being asked (Creswell, 2003; Hair, et al., 200 here 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, 1989, p. 20).

The researcher adopted mixed method research approach to examine the effectiveness of the airline credit card sales management system to convergence across qualitative and quantitative methods (triangulating data sources). Employing this approach will neutralize or cancel the biases (limitations) of applying any of a single approach and a means to offset the weaknesses inherent within one method with the strengths of the other method (Creswell, 2003, pp. 15 & 217).

In addition, adopting of mixed method research approach in this research will provide 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, pp. 12-22). This research approach will pose the researcher to the challenges for the need for extensive data collection, the time- intensive nature of analyzing both text and numeric data, and the requirement for the researcher to be familiar with both quantitative forms of research (CRESWELL, RESEARCH DESIGN, 2003)

Concurrent procedure will be employed in undertaking this research i.e. converging quantitative and qualitative 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

3.3 Target Population and Sampling Frame

3.3.1 Target Population

The population sample of the research will be the five years data of the airlines sales and the fraud rate (losses from credit card sales) of these years. The total population size is 738 including all who are working either on ticket sales, chargeback handling, accounting of credit card sales and staff working oversees. And out of the total 738 people the researcher purposely draw a sample of 160 from all these groups to get rich evidence. In addition thru the data collection instruments sample of about 160 respondents from different divisions of Ethiopian Airline has also been

Stratified Sampling technique is used for this study is to in which the entire population is divided in to technical, operational and operational strata. Sample has been taken from each division and target to reach as many as respondents in all area, the data collection was successful as the respondent count reaches 78% and 80% as shown below

Table 3.1 Distribution of respondents and non- respondents

Target group	Target number of respondents	Actual number of respondents	Non respondents	Respondents in (%)
Operational staffs	100	78	22	78%
Technical staffs	45	36	9	80%
Management staffs	15	12	3	80%

3.3.2 Sampling Frame

The sampling frame is the list from which the sample is selected, so the quality of the sampling frame affects the quality of the sample. This study intends to use a Case Study type of research design, which will focus on Ethiopian airlines enterprise credit card management system efficiency. Operational staffs who work for the airline, the management officials, or back

office employees who worked at least one year and above are expected to have sufficient and quality responses (see Table 3.1)

To meet the major objective the researcher uses purposive sampling method of draw the sample from the population. Accordingly the sample is taken based on the credit card sales volume and chargeback rates

3.4 Instruments of Data Collection

Secondary data from Ethiopian airlines data base is deployed for the analysis of the research. In addition 10 years data is also available in the central archive of the company and it is also be one part of the secondary source. The researcher will use personal interview with employees from Ethiopian credit card desk, E-commerce and from the Accounting department furthermore the researcher will also interview foreign partners of Ethiopian airlines on some specific cases

3.4.1 Data analysis and procedure

The facts and figures collected are analyzed and interpreted in qualitatively manner by comparing the company's real practice with the payment industry and control standard given by accredited government bodies like FAM (US foreign affairs manual)

Instrument

This study uses mainly primary sources. Questioner and semi structured interview are manipulated in the course of data collection. The interview guide has three parts

Part I Comprises personal employment information like the interviewee's experience in the Ethiopian airlines credit card sales process.

Part II: Comprises general information like, educational background, attitude to the current credit card handling practice and career plans.

Part III: Comprises other discussion issues like challenges faced in the credit card desk

To examine the effectiveness of credit card sales management practices at Ethiopian Airlines and identify the main problems and challenges, data are obtained both from primary and secondary sources.

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, RESEARCH DESIGN, 2003); and this method is important for collecting large amounts of raw data using question and answer style. The survey was conducted via self-administered questionnaire from the purposely sampled officers and

randomly taken operational staffs; for questionnaire is a common place instrument for observing data beyond the physical reach of the observer (Leedy, 1989, p. 142).

Questionnaire:

The questioner has been deigned under three themes the first one is organizational theme which intend to measure the company's stand point as an organization in terms of management understanding towards chargeback threat, organizational policy and procedure. The second theme is operational theme which focuses on the customer service agent awareness and competence in terms of fraud screening and fraud detection. The last one is technical theme this part of the questioner is designed with the purpose of assessing the company's system efficiency and charge back management process

Interviews:

Semi structured interview is also employed to gather more information from selected 10 commercial, IT and finance officials who frequently involve on reporting, quarterly meetings with acquirers and experienced management staffs.

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 et al., 2006). Moreover, the airline is operating in many countries across five continents and it is difficult for the researcher to reach customers at all of these airports.

3.5 Data Organization and Analysis

Like the questioner the analysis of the research is organized at three levels which are at organizational, operational and technical levels. The researcher hypothesize that chargebacks are born out of fraudulent transaction and poor system control. The researcher analyzes the collected data thru examining, categorizing, tabulating and recombining the evidence, to address the initial proposition of a study. Further the researcher analyses the data collected through survey. The data collected via questionnaires were analyzed with descriptive statistic using statistical package for social scientists. Furthermore, Wolcott (1994) as cited in Creswell (2003, p. 182), suggested that qualitative research is fundamentally interpretative i.e. the researcher shall interpret the qualitative data. Thus, data to be collected from the interview and reviews of documents and system were interpreted qualitatively. In sum, the analysis of quantitative data and interpretation of qualitative data were combined to seek convergence among the results (Creswell, 2003, p. 222).

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

This chapter presents the analysis of the collected data from various divisions of the airline who directly involve in credit card transaction. The data is presented according to the transaction flow starting from card acceptance procedure to final control mechanisms done by finance department. As indicated in the introductory part of the paper, statistical package for social science (SPSS) application has been applied to analyze the data. The descriptive analyses were also supported by the open-ended responses given during the collection of data, interview responses, reports, and literature reviews.

The researcher designs the questioner under three theme these are operational theme, technical theme and organizational theme. Accordingly the analysis is also designed on three sections

4.1 Characteristics of Respondents

The sample respondents are composed of three main areas namely from marketing these staffs are the first line employee in credit card transaction and their reply help to assess how the operational staffs accept card and detect fraudulent transactions. The second category includes business experts, strategic office and management staffs this help to see how the airline manage and understand the threat of fraud at organizational level. The last group of respondents include information security experts, back office finance analysts, and accountants who actually handle fraud loses and charge backs

4.2 Structure, policy and standard compliance towards credit card sales (Organizational theme)

Credit card transactions are mainly handled by treasury department of the airline, but considering the nature of the business the company procedure manual the defined the below parties as stake holders of credit card management system:

1. E-commerce
2. Director Treasury
3. Manager Receivables & Collection Control
4. Manger General accounting
5. Airports and area Offices who sales in credit card (this include worldwide sales offices)

The airlines use orchestrated internal procedures to define and manage the handling of credit card transaction process flow. All selling agents use system called Sabre to process credit card sales and the sales will pass thru the payment clearing company and then the payment will be transferred to the company's account

4.2.1 Compliance to international standards and internal corporate policy

As discussed in the literature review part almost all schemes (like VISA and Master) produce an industry best practice standard which should be used by any company that wishes to transact in credit card. Front line agent's competence, knowledge and understanding of fraud consequence affect the company's exposure to fraud and chargeback. Internal procedure and policy is another factor that determine the chance of fraud occurrence; the stronger the control the lesser the fraud risk will be.

The below tables show the mean of the respondent's reply in terms of the front desk agents competence, the company's procedure and policy provisions towards credit card fraud. The operational theme is summarized in to three basic parts

Table 4.1 Human capital competence and company procedure

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
EAL employees are competent enough to detect fraudulent transaction	198	137	89	110	148	682
Mean	18.0	12.5	8.1	10.0	13.5	62

Table 4.1 summarizes how much the employees are competence towards detecting fraudulent transaction on the card acceptance procedure. The mean shows that out of 62 respondents 18 believe they are not competent enough to detect frauds

On another parameter the mode for the same list of request confirm 61.2% of the respondents (i.e 38 of 62) have never had training regarding fraud detection.

Table 4.2 Card acceptance procedure

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
EAL's fraud detection procedure is best in terms of safeguarding the sales	168	105	94	75	116	558
Mean	18.7	11.7	10.4	8.3	12.9	62

The summary of table 4.2 present how strong is the company's procedure towards fraud detection, accordingly the mean computation shows that 18.7 for the strongly disagreed which is the highest of all the remaining scales

Table 4.3 Corporate policy towards fraud protection

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
Ethiopian airlines has a corporate which is capable of protecting the company from fraud loss	23	25	24	23	91	186
Mean	7.7	8.3	8.0	7.7	30.3	62

Source: Survey data

In terms of policy most of the respondents know about the policy even the highest mean value is accounted for the strongly agreed liker, it took 48.8%. the remaining respondents took the disagree and neutral options, from further interview data the respondent confirm there is no clear division of responsibility among division which may cause roll confusion

4.2.2 Ethiopian airlines credit card management system efficiency

Efficient fraud screening tool ensure the merchants to do a secured credit card business. On the below analysis the system efficiency is measured in terms of fraud detection capacity and charge back defense. It vital to rely on system than agent performance, whilst in Ethiopian airlines case 66.6% of the respondents replied that the airline does not have fraud screening solution for all channel. The researcher further refine the data and learn that the MOTO channel is still left for manual screening and no fraud tool is put in place

Table 4.4 Ethiopian airline’s efficiency on credit card handling system

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
EAL's fraud screening tool is efficient and can protect the company's sales from regardless of the sales channel	198	143	123	143	113	720
Mean	9.9	7.15	6.15	7.15	5.65	36

Source: Survey data

From table 4.3 above the mean value for the “strongly dis agree” liker took the highest value which confirm the weakness of the fraud screening system. On another parameter out of the total respondents 17(or 47% of them) believe the airline fraud rate increases from time to time. But in contradiction out of the 36 respondents 16 of them (or 44.4%) confirm Ethiopian has efficient fraud alert system. All in all the table shows the company is still far behind from the fraud risk it face

4.3 Ethiopian airlines Credit card sales (Operational theme)

Operation is the best control point to detect fraudulent transactions, the operation procedure need to be backed by strong corporate policy, technology and competent human capital. Rules and benchmarks given by schemes also focused on card acceptance procedure to make a proactive action towards fraud

4.3.1 Ethiopian airlines card acceptance procedure and the scheme rule

With the interest of protecting customers and merchants from fraudsters’ international schemes produce guidelines and periodic journals. Adherence to these standards seems to be option less for companies who want to accept branded card types like VISA and Master

Unprotected business practice will push merchants to enter in to assessment programs designed by these schemes. The assessment usual focused on the card acceptance procedure and fraud screening practice of the merchant, failure to comply to the rule and excessive charge back count on VISA card for example may lead to penalty up to USD 20,000 a month to the merchant. So it is very important to ensure the daily operation adhere to the standard set by the scheme

4.3.2 Fraud screening in Ethiopian airlines

The ideal point of screening fraud is before the customer purchase any product. Unfortunately most of the fraud screening tools availed by the payment industry detect fraud after authorization which is after the fraudster take the product or uses the service

Throughout the survey some respondents mention they never heard of the PCIDSS standards and don’t believe on the security of the card transaction. Form table 4.5 below the highest mean value goes to the “strongly disagree” liker which question company’s compliance to this standard. 33.79 mean out of 78 (which is 43.3%) respondents for such sensitive require detail investigation, accordingly from the interview some of the respondents found to be more experts o these standards.

Table 4. 5 EAL compliance to card schemes standards

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
EAL card acceptance process is made with a maximum security that can fulfill the PCIDSS standards	473	155	88	101	275	1092
Mean	33.79	11.07	6.29	7.21	19.64	78

Selling agents should have overhand on the counterfeit transactions presented by bad payers, the control point relay on the process of the card acceptance. From the below

table 4.6 the highest mean goes to the “strongly disagree” liker which accounts 39.5%. on another parameter the median 33 of the 78 (42.3%)of the operational respondents confirm that they cannot detect counterfeits during card acceptance

Table 4. 6 fraud screening tools strength

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Total
EAL fraud screening tool is strong and can counter balance the fraud risk	216	124	62	60	84	546
Mean	30.86	17.71	8.86	8.57	12.00	78.00

Source: Survey data

4.4 Technical and system issues towards credit card acceptance and charge back management

This part of the analysis focused on technical issues of the company’s credit card sales performance. Secondary data like annual reports and other confidential information (gathered in percentage format) have been taken in to account

It is important to note that charge back data is highly confidential for any company. Data like chargeback/ fraud rate directly affects stake holder’s trust over the company and may be considered as black mailing the company to other competitors. Accordingly as explained in the limitation of this research this information is encrypted in percentage form only

4.4.1 Fraud rate and sales volume

From the interview survey most respondents agree that the airline business is seasonal by its nature, which is affected by tourist movement, pilgrimage (like Muslims pilgrimage to Mecca) and international trade fares.

The sales volume of EAL increases from time to time at the same time the fraud count increases. The analysis shows higher volatility on the fraud count for example on March 2014 the fraud rate was mounted to 101% and then dramatically dropped down to 60% in addition another hiking on Aug2014 is also witnessed

As shown on table 4.4 and table 4.5 the charge back growth rate is highly volatile across the period this is mainly caused by the nature of the business, which is pick on April may July and August and slack on Oct, Nov and Dec

Table 4.4 Charge back growth rate in 2013

2013									
Month	13-Sep	13-Oct	13-Nov	13-Dec	14-Jan	14-Feb	14-Mar	14-Apr	Average
Percentage change of fraud to sales ratio (%)	47%	-42%	2%	36%	38%	-43%	101%	-60%	10%

The sales to fraud ratio shows higher ratio on March and lowest on April but all in all the average growth rate shows 10%, which means the fraud count is increasing by 10%

Figure 4.1 percentage change of fraud ratio, 2013

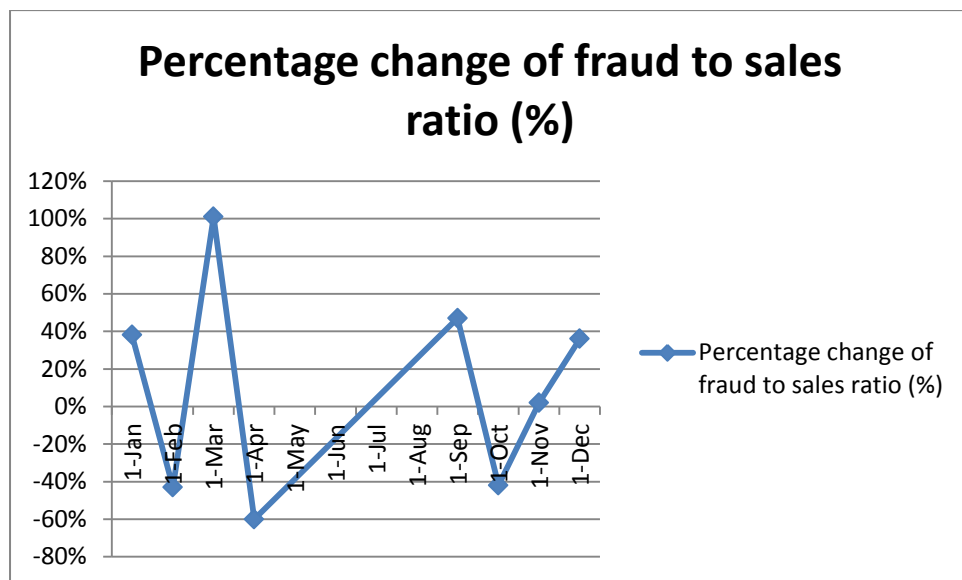
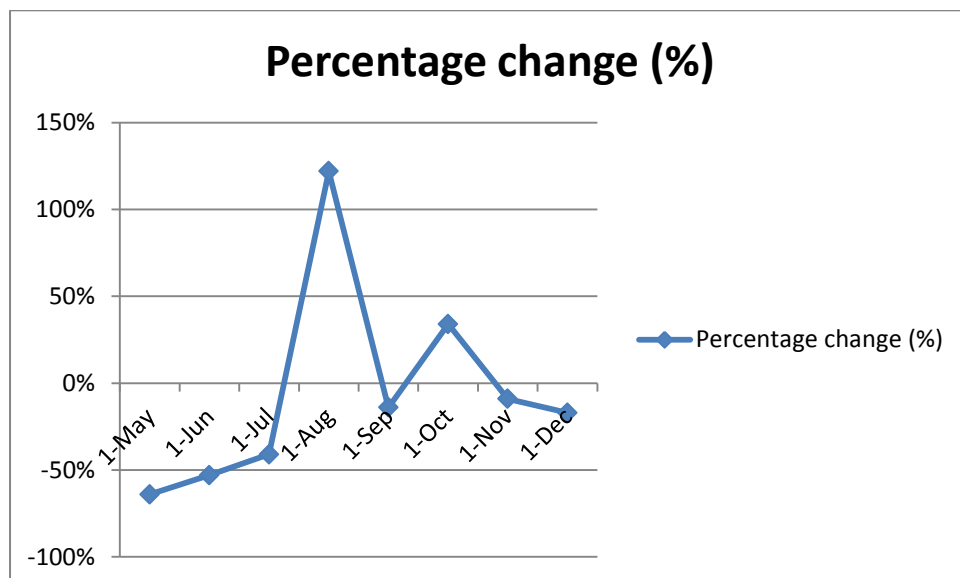


Table 4.5 Charge back growth rate in 2014

2014									
Month	14-May	14-Jun	14-Jul	14-Aug	14-Sep	14-Oct	14-Nov	14-Dec	Average
Percentage change (%)	-64%	-53%	-41%	122%	-14%	34%	-9%	-17%	-5%

For 2014 the sales to fraud ratio shows a declining rate when compared to the year before(2013) as shown on the table 4.5 above the average growth rate shows -5% which means the fraud rate is dropping down, especially on the last months of 2014

Figure 4.2 percentage change of fraud ratio,2014



4.4.2 Fraud rate in card present and card not present transactions

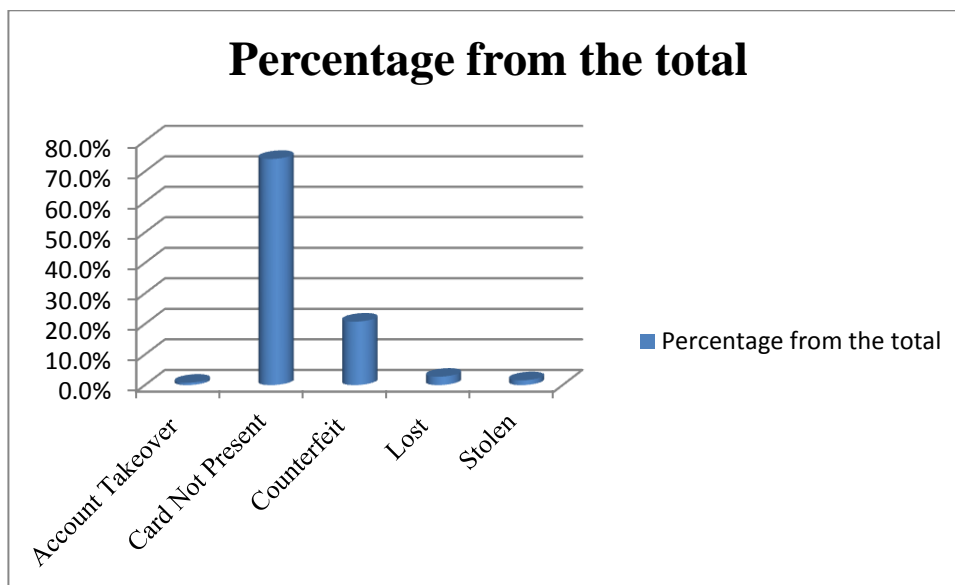
The nature of each selling channel directly related to the merchants exposure to fraud. Guidelines by card schemes and periodic articles released by anti-fraud organization argue that card not present transactions has a higher fraud exposure than card present transactions

Table 4.5 Fraud type distribution

Fraud type	Percentage from the total
Account Takeover	0.80%
Cardholder Not Present	74.10%
Counterfeit	20.80%
Lost	2.70%
Stolen	1.60%
Total	100%

From the total fraud count 74.1% of the fraud comes from card not present transactions, card not present transactions includes web site sales and MOTO (mail order/ telephone order) sales. Counterfeit or forgery is the second biggest reason for fraud to EAL which account 20.8% from the total fraud count. As discussed in the literature experts can detect counterfeit cards by manual verification, on same way they verify national identification

Figure 4.3 Fraud type distributions



As shown on Figure 4.3 the fraud rate is higher on card not present sales where there is no manual inspection and screening on the cards. From the sample interview with management members this channel (MOTO) all card sales are left with remark for manual inspection at the airport but still the fraud rate for this channel shows more than 70%

4.4.3 Charge back response time

Studies made in the payment industry shows that merchants need three to six weeks to get fraud alerts from the date of the transactions (Ethoca). It ideal to detect and take action on chargeback the moment it is raised, however the current practice shows an average of 32days to find out and defend any dispute raised on merchants

Table 4.6 Charge back response time

	Weeks	In day
Min	3 Weeks	3*7 = 21
Max	6 Weeks	6*7 = 42
Total	-	63
Average	-	31.5


Delay in action is as good as accepting the charge back loss that means the merchant should have the fraud data as fast as possible. This may depend on several factors including the merchant’s internal process. In the case of Ethiopian airlines 70% of the

charge back cases are received before 21days, and 12% of the disputes are received before the average period of 32days.

In some instance one day can be enough for fraudsters to consume the product and cause loss to the merchant. The below table shows percentage distribution of notification period for chargeback from the date of the actual sales, the worst case scenario lies on the “after 42 days” three these are cases which are received probably after the customer uses the service

Table 4.7 Chargeback notification period

Chargeback notification (from the date of the transaction)	Percentage
Before 21days	70%
Before 32 days	12%
Before 42 days	7%
After 42 days	11%
Total	100%



Fraudsters usually wish to consume the ticket before the genuine card holder find out about the charge. So the faster the information the lesser the probability if charge back loss will be

4.4.4 Fraud rate across region

Fraud exposure vary from region to region even it vary by cities of the same country, out of 80 plus destinations of the airline some of areas account very low fraud incidents. Gulf region for example account 1% of the total fraud count

Table 4.8 Charge back distribution by region

Card Issuing Region	Charge back volume percentage
Africa	5.50%
Asia (southern)	8.30%
Australia	6.00%
Europe	7.30%
Gulf & middle east	1.00%
North America	70.00%
South America	1.80%

Analysis on table 4.8 above shows that cards issued in North America account for 70% of the total fraud cases, which is far beyond the sum total of the remaining regions. Further from the interview survey with the sales agents and back office analysts it is confirmed that most of these sales originate from US issued cards.

Figure 4.4 Chargeback volume percentage by region

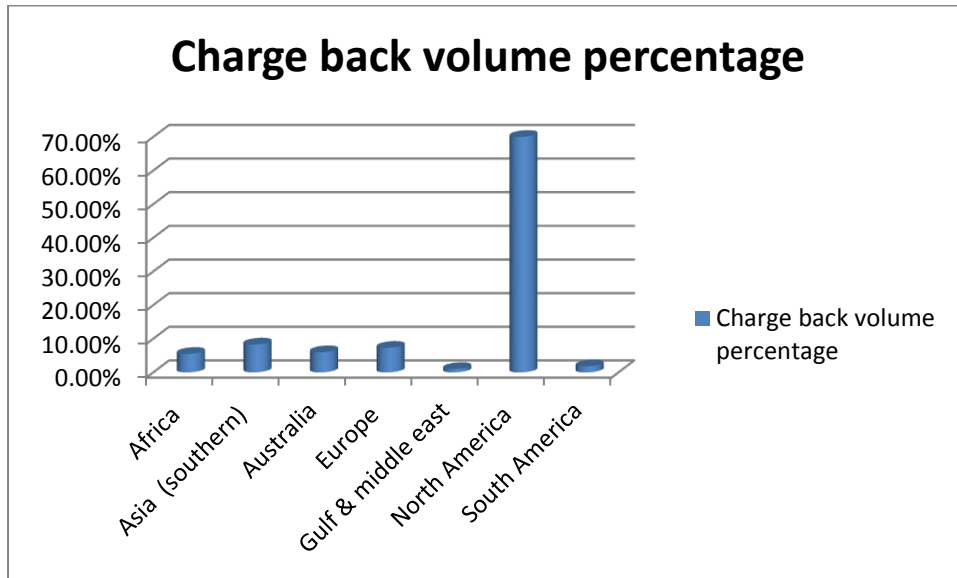


Figure 4.8 presents the graphical composition of the table, North American issued cards are still the most risky cards to transact with. Further from the interview survey, most of the travels are made from Congo to Belgium and France.

CHAPTER FIVE

FINDINGS, CONCLUSION AND RECOMMENDATION

Based on the analysis of the questioner data and the interview the researcher present the findings and conclusion of the research on this chapter. And also referring benchmarks given by the accredited institutes against the current practice of the airline the researcher forwarded recommendations.

5.1 Summary of Findings

The main objective of this thesis is to evaluate the efficiency of Ethiopian airlines credit card management system and point out the problem area that seeks attention and improvement. Accordingly the following major findings were obtained on the basis of the analysis:

- ❖ Charge back on credit card transactions is a threat to the company and charge back count can result it actual financial loss to EAL. This threat is aggravated by the weak control system during card acceptance
- ❖ Ethiopian airlines fraud rate is increasing from time to time which is fueled by increase sales volume and the contemporary facts of the payment industry. The fact that EAL operate in Africa contribute its part to the hiking on fraud counts
- ❖ From the total fraud count it is confirmed that most of the charge back comes from North America, Europe and West Africa. From the interview agents confirmed that most of the frauds are made on a round trip bookings from west Africa to Europe like from Congo to Belgium and France
- ❖ EAL uses fraud detection strategy that enable fraud detection after issuance of ticket which is usually called “ after the transaction strategy”
- ❖ Most of operational staffs cannot manually identify whether the cards presented to them are counterfeit or genuine. From the interview 70% of the operational staffs confirmed that they never had any training about credit card security. EAL’s has management policy that enable fraud screening and PCIDSS compliance which can satisfy the requirement of the card schemes and other anti-fraud institutions and governments need
- ❖ Technically all charge back does not cause actual financial loss to merchants, however in EAL case the company losses significant amount of money due to charge backs. Further interviewee confirmed that charge backs also spoil sets in travel industry
- ❖ Transactions made on North American issued cards account 70% of the total fraud count of the airline but the airline does not have any special treatment for this cards

- ❖ From the interview the researcher confirmed that fraudulent transactions can be caught after issuing an air ticket. This way of fraud monitoring is known as “after the transaction strategy” which is currently used by EAL

5.2 Conclusion

Based on the analysis result and the findings the researcher draw the below conclusions which can reflect the current state of Ethiopian airlines credit card handling system

- ❖ Ethiopian airlines is losing its sales due to weak fraud screening tool the research finding and the numerical figure on the analysis all confirmed that the current tools deployed by the airline does not protect the company’s sales, as it should
- ❖ There is a training gap specially for operational staffs the researcher measure there competence against the industries best practice and witnessed they are not competent enough to the level that can assure the airline to make a secured credit card business.
- ❖ The volume of fraud found to be concentrated in some regions and on some card types mainly issues from North America. The data collection thru interview confirm the region to be the most risky business area for EAL and it is imperative to conclude that North American cards are increasing fraud exposure of Ethiopian airlines from time to time
- ❖ EAL is exposed to fraudsters target like all airlines but does not have a defined fraud detection and charge back management section which can update the company with the industry’s dynamism and counter balance the fraudster act
- ❖ The “ after the transaction strategy” expose the company for a number of fraud counts which were easy to stop before happening in the “before the transaction” strategy
- ❖ ET’s selling strategy concentrate mostly on credit cards and show a minimum effort towards other options like mobile payment which are highly recommended by payment industry specialists and also confirmed to be the most secured option than credit cards

5.3 Recommendation

After benchmarking the best industry standard and considering the current practice of EAL, pointed in the finding section of this chapter, the researcher developed the below recommendation and corrective actions to be taken for management and technical decision by the airline

- ❖ Ethiopian airlines should add more fraud screening tools to its card acceptance process to strengthen the internal control system. Similarly EAL should also encourage the use of magnetic readers or point of sale terminals for all face to face transactions. This will ensure the company’s compliance to PCIDSS standards where by the fraud exposure will significantly decreases
- ❖ As shown in the analysis and finding there is a knowledge gap specially for EAL’s operational staffs who directly contact the fraudster. As a big opportunity the company has its own highly accredited aviation training center, so a recurrent training program should be designed to build

Credit card management system: special emphasis on Ethiopian airlines

capacity. It is also helpful to persuade section managers to train their agents before assigning them on credit card sales and card verification process

- ❖ It is important to note all these incidents happened due to credit card sales, so as a commercial strategy the company needs to consider another more secured payment option like availing mobile payment to its sales outlets. Moreover, the industry has introduced a brand new payment solution like Apple Pay, Google Wallet and a few other services which use a wireless technology called near-field communication (NFC). These technological products are far better than credit cards in terms of payment security and convenience
- ❖ The airline needs to categorize the whole credit card sales by country, card type and other features to point out highly risky card types or countries. This enables the company to separately treat sales made with specific cards or transactions that originate from a specific country. Accordingly, the company can add an additional security layer to mitigate fraud risks or even to revoke card payment from highly risky countries or card types

Bibliography

- Airlines Reporting Corporation(ARC). (2010). Credit Card Acceptance & Chargeback Prevention. *Tips for Travel Agents*, 10.
- Associated Press (AP). (2015, Feb 16). Global gang stole bank funds from 100 institutions, but untouched customers still at risk. US.
- BWA Merchant service. (2012). Credit Card Fraud Protection– User Guide. *User Guide*, 9.
- Capital. (2012). The Ethiopia Observatory. *The Ethiopia Observatory*, by Muluken Yewondwossen.
- CIMA(chartered institute of management accountants). (January 2009). *Fraud risk management, A guide to good practice*. London SW1P 4NP.
- CImA, A guide to good practice, p.14. (2009). *Fraud risk management. A guide to good practice*, 14.
- Cressey, D. R. (1973). The Fraud Triangle originated from Donald Cressey's hypothesis. *Other People's Money*, 30.
- CRESWELL, J. W. (2003). RESEARCH DESIGN. In J. W. CRESWELL, *RESEARCH DESIGN, SECOND EDITION* (p. 153 to 154).
- CRESWELL, J. W. (2007). RESEARCH DESIGN. In J. W. CRESWELL, *RESEARCH DESIGN, SECOND EDITION*.
- Dara, J. (n.d.). Credit Card Security and E-payment. *Enquiry into credit card fraud in E-Payment*, 10.
- EDWARD, B. b. *LOOKING BACKGROUND*. 1987.
- Engadget. (n.d.). *Engadget.com*. Retrieved from <http://www.engadget.com/>: <http://www.engadget.com/>
- Engadget, <http://www.engadget.com/>. (n.d.). *Engadget.com*. Retrieved from <http://www.engadget.com/>: <http://www.engadget.com/>
- Ethoca. (n.d.). *Ethoca solution*. Retrieved from ethoca.com: <https://www.ethoca.com/solutions>
- Guardian, T. (2014, Dec). Kenya arrest 77 Chinese national in cybercrime raids .
- Idea Works, C. (July 2014).
- LexisNexis. (2013). True Cost of Fraud. *Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud*, 5.
- National bank of Ethiopia . (2012, May). <http://www.nbe.gov>. Retrieved from <http://www.nbe.gov.et/aboutus/faq.html>
- NILSON, c. e. (2013). *Personal consumption expenditure*. Washington D.C.
- Porter, M. E. (n.d.). *COMPETITIVE STRATEGY*. New York: THE FREE PRESS.
- Research, J. S. (2008 , Dec 9). *Javelin Strategy & Research*. Retrieved from <https://www.javelinstrategy.com/news/592/91/Online-consumers-will-use-credit-cards-less-often-report-predicts>
- United States Federal Trade Commission, Consumer Sentinel Network, U.S. Department of Justice. (2014). *Credit Card Fraud Statistics*. Washington DC: United States Federal Trade Commission.
- Visa International Best Practices Guides. (2014). Visa International. *Visa International Best Practices Guides*, p. 16.

ANNEXES

ANNEX I Questioner

St. Mary's University
School of Graduate studies faculty Business and
Economics
Department of Accounting and Finance

Dear respondent

In partial fulfillment my of masters' degree in Accounting and finance I am undertaking research on the current credit card management of Ethiopian airlines enterprise. Accordingly I have prepared this questioner survey to further analyze and come up with better recommendation for the company and other stake holders. This survey will assess and measure the technical, operational and organizational issues in handling credit card transactions in Ethiopian airlines

Your honest response to each question will help to meet the general objective of my research, the questioner may take you 20min and it will be used ONLY for academic purpose. Hence all respondents will be kept in strict confidentiality so that it will not affect any one in any case

I would like to thank you for your time and kind participation in this survey and timely response to this questioner

Many thanks,

Abraham Zerihun

General instruction

This questioner has three parts with a total of 56 questions referring to your actual experience the last part is to be filled if the researcher misses any point which should be raised

Please answer all questions with respect to the current credit card management and practices in your section; please reflect your view on the current process flow of the credit card transaction not on the past or the best industry standards. Your honest response will contribute to find out the problem and come up with a valid conclusion and recommendation

Please circle the appropriate response on the question using the following likert scale

1 = strongly agreed

2 = Agreed

3 = Neutral

4 = Disagree

5 = strongly disagree

Part I. Demographic information

Please use "X" to indicate your selection from the below demographic information

Section

E-commerce		Call center		Ticket office		Airport		Others	
------------	--	-------------	--	---------------	--	---------	--	--------	--

Your job responsibility/ title

Operational		First line supervisor		Manger & above	
-------------	--	-----------------------	--	----------------	--

Your Experience in Ethiopian airlines

1 to 3 years		4 to 6 years		> 6 years	
--------------	--	--------------	--	-----------	--

Part II. Credit card handling practice at EAL

A. Technical Theme

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	EAL has fraud screening tool to secure all its selling channels					
2	Fraud prevention procedure used by EAL is enough to make a secure credit card business					
3	Fraud rate in EAL is decreasing from time to time					
4	The financial risk of credit card is monitored					
5	EAL has structured, efficient and knowledgeable department to support operation staffs on credit card related issues					
6	Credit card fraud alert system support area offices 24/7					
7	EAL has fraud protection tools for each selling channel					
8	EAL's fraud protection tools are efficient and are updated in line with the fraud risk of the industry					
9	EAL has efficient system to transmit fraud alerts across divisions and take immediate action					
10	EAL has a knowledge sharing system about fraud detection best practices					
11	EAL has efficient control over its credit card sales					
12	Ethiopian airlines fraud risk is higher than the industry average					
13	Ethiopian airlines has efficient charge back alert system					
14	EAL uses Velocity Checking to screen fraudulent transactions					
15	EAL uses Geo-location Checks to screen fraudulent transactions					
16	The current fraud screening tools deployed are					

	not strong enough to protect EAL's credit card sales					
--	---	--	--	--	--	--

B. Organizational theme

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Internal control of EAL towards credit card transactions is strong					
2	EAL is efficient in terms of controlling and accounting credit card sales					
3	EAL make fraud risk analysis for internal and management consumption					
4	EAL has a defined section to support operational stuffs					
5	EAL losses money due to chargeback and fraud					
6	Charge back loss is insignificant for Ethiopian airline and should not be an issue					
7	EAL has a clear management policy towards credit card fraud management					
8	The management policy of EAL clearly define the roll of each division on credit card sales handling					
9	EAL has a corporate policy to prevent fraud					
10	EAL has well organized credit card office that navigate the business environment and update operational stuffs about how to make a secured business					
11	EAL management know the true cost of fraudulent transactions					
12	Ethiopian airlines policy on fraud detection is updated every time to effectively battle charge back and fraud					
	Fraud is something which we cannot avoid in airline business and I believe EAL should accept it as business risk					

14	The roll and responsibility of all divisions in respect to charge back handling is clear					
----	--	--	--	--	--	--

C. Operational theme

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Fraudulent transactions can detected easily					
2	All cards in credit card transaction are encrypted/masked by the system					
3	Ticket verification at the airport is NOT important for every card not present transactions					
4	My immediate supervisor knows the volume of charge back we receive every day					
5	My immediate supervisor remind me to follow procedure to avoid charge back losses					
6	There is a recurring training for operational and back office staffs about credit card security and fraud privation					
7	Fraud detection tips are usually disseminate so that we will be capable of detecting fraud					
8	My immediate supervisor discuss with me about the fraud rate and possible solutions					
9	I am fully aware how fraudulent transaction affect EAL's sales					
10	I fully understand what is expected from myself to protect the sales from any charge back					
11	I know the major reasons for charge back and fraud					
12	I don't know how I can detect fraudulent transaction					
13	I know what PCIDSS standard is and my immediate supervisor ensure compliance to this standards					

14	Before issuing any ticket I always check card expiry date and cross check name from the passport					
15	I always swipe card in magic reader while issuing ticket (for CTO & ATO staffs only)					
16	We retained copy of signature authority for all credit card sales before accepting passenger for any flight					
17	I can access the full credit card number at the time of issuing the ticket					
18	I can access the full card number whenever I want					
19	We use UCCF form for all face to face transactions (for CTO & ATO staffs only)					
20	I know fraudulent transactions will cause a pure loss to the airline					
21	Some selling offices compromise card verification to satisfy the customer need					
22	Some agents are negligent on the risk of fraud					
23	I use fraud screening tool for every sales					

Part III. Open-Ended Questions

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

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

AVS

Negative Databases

CVV2

Verified by Visa

Credit card management system: special emphasis on Ethiopian airlines

Velocity Checking

Fraud Detection Tool

Geo-location Checks

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

Excellent

Very good

Good

Poor

Very Poor

===== Completed =====

Annex II Personal consumption expenditure prediction by Nelson

Personal Consumption Expenditures in the United States (Tril.)



* Includes food and lodging received by employees including those in domestic service ... food and fuel produced and consumed on farms ... rental value of buildings and equipment owned by nonprofit organizations serving individuals ... financial services furnished without payment (except life insurance), expense of handling life insurance and pension plans, brokerage commissions on certain securities ... owner-occupied and rented farm and nonfarm housing ... employer contributions for group insurance ... and clothing issued to military personnel.

©2013 The Nilson Report

Annex III High fraud count by regions

