2006:23

MASTER'S THESIS

Credit Card Security and E-payment

Enquiry into credit card fraud in E-Payment

Jithendra Dara
Laxman Gundemoni

Luleå University of Technology

Master Thesis, Continuation Courses
Computer and Systems Science
Department of Business Administration and Social Sciences
Division of Information Systems Sciences

2006:23 - ISSN: 1653-0187 - ISRN: LTU-PB-EX--06/23--SE

ABSTRACT

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

Credit card frauds come in several ways. The most prevalent and commonly known type is counterfeit card fraud. 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 which accounts for higher percentage of frauds in electronic payment in most developed countries. However, as new banking channels have opened up, for example internet, phone banking and e-commerce, and the boom in credit card use, crime has migrated to seek any opportunity to attack these new and immature transaction methods. Our study is an attempt to ***delve a*** little further into the issue of credit card frauds by exploring the processes involved and pursued by two financial institutions in Sweden and India, focusing on the four key processes identified by Buttfago and Dyxler.

Keywords: *Electronic Payment, Credit Card, Counterfeit fraud, Cardholder-Not-Present.*

DEDICATION

I wish to dedicate my Master Thesis to my Parents, Brothers, and my dear friends who supported me to study in sweden and encouraged me in all crucial situations. I am heartly thankful to all who helped in pursuing my Masters Education.

------------------------- ***Laxman.Gundemoni***

I dedicate my thesis work to my Mom , Dad and Brother. My special thanks to my friends close to me. I would like to give the greatest of thanks to my family for always being there when needed, and constantly taking so extremely good care of me.

-------------------------------- **Jithendra Dara**

ACKNOWLEDGEMENT

This study was performed as our Masters thesis during the end of 2005 and in the begining of 2006. Throughout the process of writing this, we have learned that writing a thesis is neither overly exciting, nor perticularly fun. On the other hand, it has been a very useful and valuable experience, and we have learned a great deal, not only about the topic at hand, but also how to manage great work load with in a limited time frame. However, this workload would not have been managable if we had not received help and support from a number of people who we would like to mention.

First of all, we would like to thank Sir, Svante Edzen for his help and supervision during the writing of the thesis. Moreover, we would like to express our gratitude to on managers who are to allocate their valuable time in order share their proffesional knowledge with us during the entire thesis period. – Thank you all!

Lulea University of Technology

Laxman. Gundemoni   Jithendra. Dara

TABLE OF CONTENTS

1.0 INTRODUCTION

This chapter will explain the background of the research study. This will guide the reader to understand the Electronic Payment System and about the credit card. And we discussed the Problem area, later we state the purpose of the research study and then research question. We also present our delimitations of our thesis. Finally the disposition of the thesis will be illustrated

1.1 BACKGROUND

"Everything must be assessed in money, for this enables men always to exchange their services, and so makes society possible". – Aristotle.

The idea of paying for goods and services electronically is not a new one. Since 1970s and early 1980s, a variety of schemes have been proposed to allow payment to be effected across a computer network. After a period of exponential growth, 930 million people have Internet access worldwide. The electronic payment system started at the end of 1996 and in the earlier part of 1997, a huge variety of different payment methods developed by both academic researchers and commercial interests. Some of these were launched on the market and failed to reach a critical mass. Cyber cash digi cash launched payment systems that achieved quite extensive deployment but failed to generate an economic return. At the same time many companies started up new methods of payments for B2C sector (Donal o´mahony, 1997).

The Electronic Payment (e-payment) is a method of value exchange in electronic commerce, where the value is transferred via the Internet and communication technologies. The electronic payment systems have evolved from traditional payment systems and consequently the two types of systems have much in common. Electronic payment systems are much powerful, especially because of the advanced techniques in security that have no analogs in traditional payment systems. An electronic payment system denotes any kind of network service that includes the exchange of money for goods or services. E-payment is conducted in different e-commerce categories such as Business-to Business (B2B), Business-to-Consumer (B2C), Consumer-to- Business (C2B) and Consumer-to-Consumer (C2C).(Donal o´mahony, 2001)

Of the security issues facing banks everywhere, prevention of card fraud has always been a high priority, and is set to grow even further in importance. (*Paul Meadowcroft, Head of transaction security of the e-Security activities of the Thales Group*)

The level of card fraud has risen significantly over recent years, caused in the main, by the explosion in the number and usage of payment cards and the associated high level of organized card crime activity. For example, over the past decade, fraud losses on UK-issued plastic cards have risen from £96.8m to a staggering £402.4m a year. And these figures do not take into account the 'soft' costs related to card fraud, such as tarnish to reputation and potential legal costs. (The Economist, December 2004).

Credit cards are the most popular payment instrument on the Internet. The first credit card was introduced decade's ago. (Diner's club in 1949, American Express in 1958). These cards have been produced with the magnetic stripes with unencrypted and read-only information. But today many cards are smart cards with the hardware devices offering encryption and far greater storage capacity.

In 1996 Visa and Master card announced that they were working together to define a protocol that would enable secure bankcard transactions on the Internet. This process involves the use of highly secure encryption digital signature techniques, as well as digital certificates. So that there is no export problem because these mechanisms are embedded in the payment process and are not accessible to the users to secure other (non-financial) information. A commonly known disadvantage is the high transaction fees associated with credit card use. (Tae-Hwan, 1998)

The most interesting event in the whole of this area has been the off again on-again liaison between Master card and Visa to produce what is becoming the de facto Internet standard for secure bankcard payments. The credit card based e-payment simply requires the provision of purchaser's credit card details to the service provider for goods and services purchased over the Internet. There are some risk involved in sending such details there is a chance to hack some one to over come this problem Master cards and Visa cards are came. The usefulness of payment by credit cards cannot be over emphasized. Among the numerous advantages are as outlined below: (Tae-Hwan, 1998)

- They allow you to make purchases on credit without carrying around a lot of cash
- They allow accurate record-keeping by consolidating purchases into a single statement;
- They allow convenient ordering by mail
- They allow you to pay for large purchases in small, monthly installments
- Under certain circumstances, they allow you to withhold payment for merchandise which proves defective.
- You don't have to pay the portion of the credit-card bill or related interest charges while the dispute is being investigated
- A credit card means you can make purchases abroad without having to worry about local currency.

Credit cards can help coordinate receipts for tax purposes. (Tae-Hwan, 1998)

1.2 PROBLEM AREA

The Internet is currently helping and facilitating online purchases and make payments very flexible. This has lead to a new market for companies on which the number of customers is frequently increasing.

According to Sandra Stammberger, Commerce and technology, combined as a one package – this is what online credit cards are. With the advent of Internet, the knowledge and communication barriers were broken. Also, with Internet, came the concept of e-shops or virtual shops that existed only on the Internet. You could shop at these shops by making use of their online credit card payment-acceptance ability. Once the online credit card payments were verified and approved, the goods got delivered to your door. This is what we call convenience at its best (EzineArticles.com, 2006)

With more and more e-shops getting setup everyday, online credit card usage is becoming even more popular. The possibility of receiving online credit card payments has given a totally new dimension to shopping. Now, you cannot only shop from the comfort of your home, you can even get discounts on these products. (EzineArticles.com, 2006).

Among the pitfalls of online credit card usage is the prevalence of online credit card fraud. This online credit card fraud can happen in several ways. Numerous types of card fraud have been developed over the years and are regularly committed throughout the world. The most prevalent and commonly known type is counterfeit card fraud. However, as new banking channels have opened up, for example internet, phone banking and e-commerce, and the boom in credit card use, crime has migrated to seek any opportunity to attack these new and immature transaction methods. (EzineArticles.com, 2006)

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 over the past couple of years, and counterfeit fraud has now been overtaken as the most costly type of card fraud by a newer method, that of Cardholder-Not-Present (CNP) fraud. In the UK in year 2004 alone, CNP fraud was responsible for losses of £116.4m – more than any other type of card fraud, in the USA, $428.2m and France recorded CNP fraud of 126.3m over the same period.(Financial Times, January 2005; UN World Report on electronic fraud-December 2004). From the afore-discussed it is evident that credit card frauds offer a wider and interested area for research or study

1.3 RESEARCH PURPOSE

The aim of our study is to find out the mechanisms that banks and other card issuing institutions put into place in order to minimize these increasing and worrying problems in credit card transactions. Among other things, we would also seek to describe the security features of the credit card and to investigate how to secure credit cards from fraudsters both on the Internet and offline transactions.

1.4 RESEARCH QUESTION

From our earlier discussion (1.2 Problem Area) above, a research question has been formulated in order to make research. This is stated as below:

Main Question.

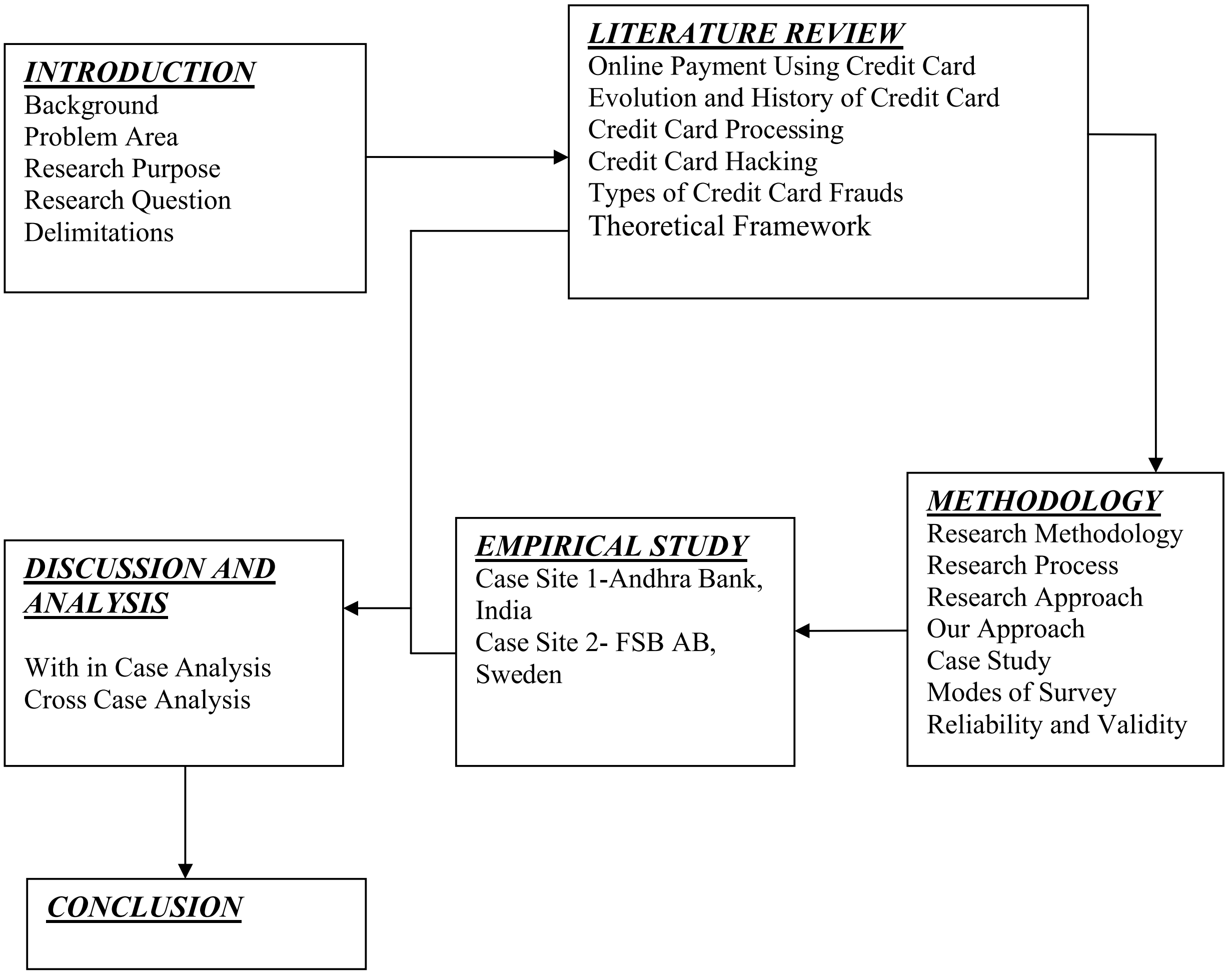
What security measures can Bank Authorities adopt to secure credit card users details?

Hence our question focuses on security measures adopted by *Bank Authorities* in securing credit card details, here our main focus or emphsis is to show the thechniques used by some advanced country.

1.5 DELIMITATIONS

The thesis focuses mainly on the fraudulent transactions involved in credit cards. There are some other ways of frauds in the credit cards, which we may not know. There are some more chances that our conclusions may be inconclusive based on the fact that this study would not cover a sizable user community of credit cards as well as card issuing companies. The study of this project can be considered to some extent for the customers who purchase the products through credit cards.

1.6 THESIS DISPOSITION



2.0 LITERATURE REVIEW

This chapter will explain how the payment is done using the credit card, and credit card evolution. We also explain the processing of the credit card system, later we discuss how credit card hacking is done in online and the different ways of hacking. And also we discuss about the frauds and fraud techniques. And later we explain the" detection and fraud prevention on the internet" which explains our theoretical fame work of our thesis.

2.1 ONLINE PAYMENT USING CREDIT CARD

"A credit card is a card that allows you to borrow money to pay for things. There will be a limit to how much you can spend called your credit limit. At the end of each month you can either pay off the whole of the amount you owe or make a minimum repayment."- Proff. Phil Edwards

With the rising interest in e-commerce, electronic payment techniques have increased more in number. The most popular way is payment-using credit card, probably because of its simplicity and comfortable. The user just enters the relevant numbers, the merchant gets these validated and payment has been made. For extra security, the communication between user and merchant should be encrypted.

Payment by credit card is the most popular and the easiest way to pay for goods and services online. A user simply enters his credit card number, his name and the expiry date of the card; the merchant validates this information and upon approval from the credit card company, ships the goods or provides access to the service. The only thing that needs to pass between the merchant and the buyer is the credit card number.

2.2 EVOLUTION OF CREDIT CARD

A credit card is a great financial tool. It can be more convenient to use and carry than cash and it offers you valuable consumer protections under federal law. However, it is also a big responsibility. If not used carefully, you may end up owing more than you can repay, damaging your credit rating and creating credit problems for yourself that can be difficult to fix.

Credit cards, as we know them today, have been around for just over half of a century. One of the first credit cards appeared in 1951 when loan customers of Franklin National Bank of New York were screened for credit and those approved were given a card they could use to make retail purchases. Participating merchants copied the customer information from the card onto a sales slip and the bank would credit the merchant account for the loan less a flat fee to cover the costs of providing the loan. In 1958, The American Express Company (a company built on the traveller's cheque business) began issuing a charge card for travel and entertainment charges, which was accepted at participating restaurant, hotel and airline merchants. (creditcards.com. 2006).

Cardholders enjoyed the convenience of plastic charge cards (especially when on the road for business) as well as the line of credit offered by the new bank credit cards. Merchants found that credit card customers usually spent more than if they had to pay with cash (which is still true today – the average credit card purchase is 112% more than if cash is used). Accepting bank-issued cards was safer for the merchant than dealing with cash (more secure from internal and external theft and error) and less expensive than creating and maintaining a merchant-specific credit program (creditcards.com. 2006).

2.2.1 Bankcard Associations

In 1959, Bank of America began issuing the BankAmerica within California, which was the first universal credit card with widespread merchant acceptance. Bank card associations began in 1966 when Bank of America formed licensing agreements with other banks. This enabled them to issue credit cards on a widespread basis and settle transactions among participating banks. (creditcards.com, 2006)

Also in 1966, a group of 14 US banks formed Interlink, a new bankcard processing association with the ability to exchange information on credit card transactions. In 1967, four California banks formed the Western States Bankcard Association and introduced the Master Charge program (which was later renamed MasterCard in 1979) to compete with the BankAmerica card (later renamed Visa in 1976) program. VISA and MasterCard are organizations that both issue credit cards through member banks and set and maintain the rules for processing. They are both run by board members who are mostly high-level executives from their member banking organizations. (creditcards.com. 2006).

As the bankcard industry grew, banks interested in issuing cards became members of either the Visa Association or MasterCard Association. Their members shared card program costs, making the bankcard program available to even small financial institutions. Later, changes to the Association bylaws allowed banks to belong to both Associations and issue both types of cards to their customers

2.3 ELECTRONIC PAYMENT SYSTEM

In order to participate in the electronic payment system the customer and the merchant should access the Internet and initially they have to register the corresponding the payment service provider. The provider in turns provides the payment gateway that can be reachable from both public network and the private interbank clearing network. Here the gateway acts as the intermediary between the traditional payment infrastructure and the electronic payment infrastructure. On the other side customer and the merchant have their bank accounts at the bank that is connected to the clearing network. The customer bank (issuer bank) actually issued the payment instrument that the customer uses for his payment. The acquirer bank acquires the payment records (Vesna Hassler, 2001).

When the customer is purchasing the goods and services, he chooses to apply through his debit or credit card. Before delivering the goods the merchant asks payment gateway to authorize the customer and his payments. The payment gateway contacts the issuer bank to get clear. If every thing is fine the payment gate with draws the money from the customer account and deposits in the merchant account and sends the notification to the merchant. Then the merchant delivers the goods and services to the customer. (Vesna Hassler, 2001).

The major reason for developing an electronic payment system is that it provides organisations and consumers with a means of integrating individual commercial services into an electronic market place. According to Tae-Hwan, 1998, Lynch and Lundquist argue companies and consumers both of them will get benefit from the e-payment system.

- Companies will benefit from virtual markets because the concept of online shopping can make their business communication easier and cheaper.
- Consumers will benefit because on-line shopping is convenient and saves time.

The types of Electronic Payment System are Offline versus online, Debit versus credit, Macro versus Micro, The paper cash, credit cards and the checks are the types of electronic payment system but newly electronic payment system has introduced two types of payment instruments:

- Electronic money (digital cash)
- Electronic checks.

Common to the entire payment instrument is the fact that the actual flow of the money from payers account to the payee account. (Vesna Hassler, 2001).

A Typical Electronic Payment System

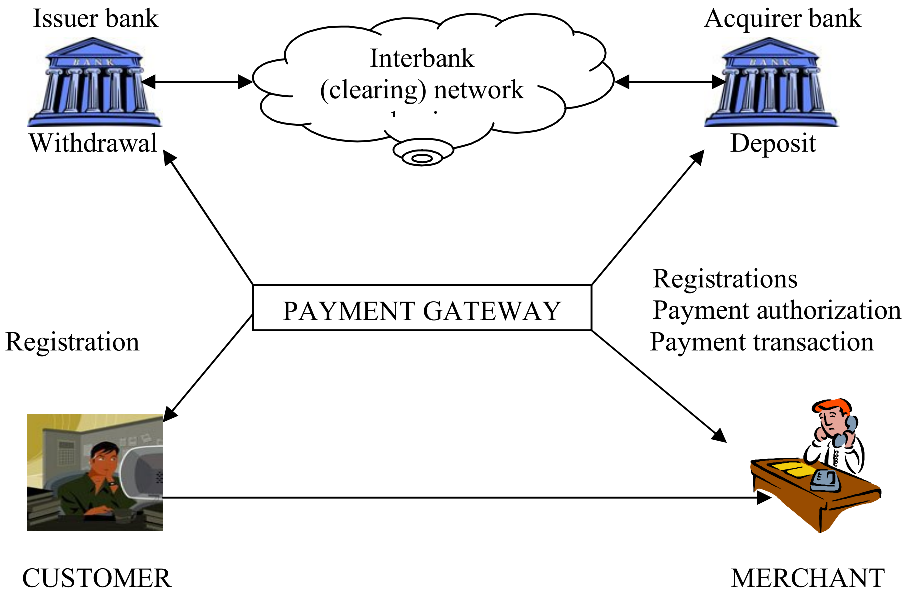


Fig-2.1 (Security Fundamentals for E- Commerce, by Vesna Hassler, 2001)

2.4 CREDIT CARD PROCESSING

As the credit card processing became more complicated, the outer service companies started to sell processing services to Visa and MasterCard 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. (creditcards.com, 2006)

The rules and standardized procedures of Visa and MasterCard are developed for handling the bankcard paper flow in order to reduce fraud and misuse of cards. The two associations also created international processing systems to handle the exchange of money and information and established an arbitration procedure to settle disputes between members.

2.4.1 Roles Involved In Credit Card Processing

Credit card processing is the process where it happens with many parties, it also referred to as roles involved in the processing of a credit card transaction. Namely, the issuer, the cardholder, the merchant, the acquirer, the card association, and the settlement bank. (Keith Lamond, 1996)

The card issuer is a licensed financial institution or its agent that issues the credit card to the cardholder and is responsible for the provision of responses to authorization requests. Those financial institutions can be a bank, also referred to as the issuing bank that is member of a card association and adopts a payment card product promoted by the card association. The issuer here keeps the cardholder accounts to which he charge the bills The issuer guarantees payment for authorized transactions, processing the payment card in accordance with the payment card product regulations and local legislation. The issuer supports the clearing and settlement functions between the cardholder and the acquirer. The issuer host is the computing system that accesses the cardholder accounts database and represents the issuer during the authorization, clearing, and settlement.

The cardholder is a customer of the issuer that uses a payment card in a B2C payment transaction. The card acceptor is the party that accepts a payment card at the point of service, formats the data of the transaction in a payment message, and forwards the payment message to the acquirer.

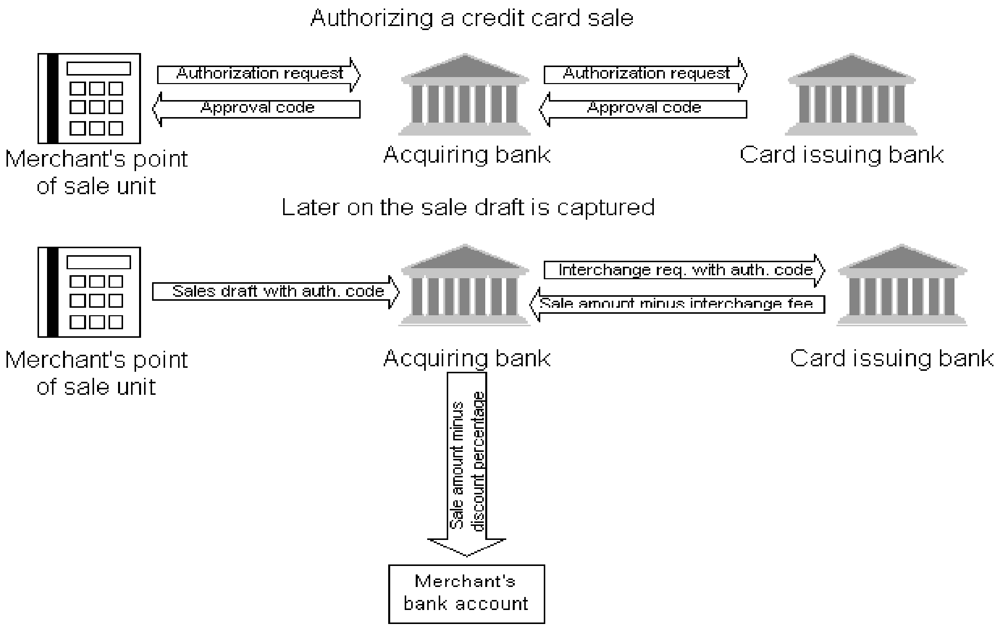

Authorizing a credit card sale
Authorization request
Approval code
Authorization request
Approval code
Merchant's point of sale unit
Acquiring bank
Card issuing bank
Later on the sale draft is captured
Sales draft with auth. code
Interchange req. with auth. code
Sale amount minus interchange fee
Merchant's point of sale unit
Acquiring bank
Card issuing bank
Sale amount minus discount percentage
Merchant's bank account

Fig-2.2 (Credit Card Transactions: Real World and online, by Keith Lamond, 1996)

2.5 CREDIT CARD HACKING

.In 1980 the term hacking became a buzzword, which was taken to be derogatory and by the misuse or overuse was attached to any form of socially non-acceptable computing activity outside of polite society. Credit card hacking is harder to do using traditional methods such as decrypting the magnetic stripes and recreating them. Hackers were assumed to be the fringe society of the computing fraternity, who did not know any better and who had obtained access to a technology with which they terrorized the world of communications and computing. These connotations are in contrast to the use of the term in the 1950's and 1960's when hackers were at least to be tolerated for their potential, though not necessarily displayed in public. Scientists such as Edison (electric light bulb, phonograph, etc.), Fleming (penicillin), Barnes-Wallis (the bouncing bomb and swept wing aircraft), Watson-Watt (radar) and possibly even Babbage (the difference and analytical engines), may have been honored to be identified as hackers. Only in more recent times has there been confusion between the terms hacker, petty criminal. (J.A.N Lee, 1991)

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. In hacking a computer, the enhancement of the system is an end in itself. Applications of that system don't count. In the same manner, 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. While hacking was generally counter-society it is not necessarily anti-society. (J.A.N Lee, 1991)

2.6 DIFFERENT WAYS OF HACKING

In an online credit card purchase, the payment data transfers between the customers PC and the vendor's shop over the internet. 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 you should see a secure site symbol displayed by the Web browser as proof. If one doesn't see evidence of a secure site, the transfer of personal information, including the credit card data, it could be exposed and subject to theft. One should be careful and should think before entering the data. Because it is difficult to intercept information transferred over a secure connection. (FSPro Labs, 2001-2005)

2.6.1 Attack a Shop to Access the Customers Database

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. Hopefully, if a site detects an attack, you might be notified in time to protect your card and prevent unauthorized charges (FSPro Labs, 2001-2005)

2.6.2 Fool Customers Into Submitting Card Information Voluntarily.

The unknown persons have 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)

2.6.3 Attack ***your PC to steal your card information –an internet explorer security breach.***

The hackers are the unauthorized user who tries to access over the internet or anyone with direct physical access can commit identity theft by stealing credit card information on PC. 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 someone accesses ones computer directly or remotely his credit card information can be stolen. (FSPro Labs, 2001-2005)

2.7 TYPES OF CREDIT CARD FRAUDS

Now a day Credit Card Fraud is the major and one of the biggest threats to business establishments. However, to overcome the fraud effectively, it is important to understand the Mechanisms of executing a fraud. The credit card fraud makes a group and employs a large number to commit fraud. In simple terms, Credit Card Fraud is defined as when an individual uses another individual's credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used. And the persons using the card has not at all having the connection with the cardholder or the issuer and has no intention of making the repayments for the purchase they done.
(Tej Paul Bhatla, 2003)

Credit card frauds are committed in the following ways: (Tej Paul Bhatla, 2003)

- An act of criminal deception mislead with internet by use of unauthorized credit card account or by getting their personal information

- Illegal or unauthorized use of account for personal gain

- Misrepresentation of account information to obtain goods or services.

It is believed more that the merchants are far more at risk from credit card fraud than the cardholders. While consumers may face trouble trying to get a fraudulent charge reversed. Merchants lose the cost of the product sold, pay charge-back fees, and fear from the risk of having their merchant account closed (Tej Paul Bhatla, 2003).

Increasingly, the card not present scenario, such as shopping on the internet poses a greater threat as the merchant is no longer protected with advantages of physical verification such as signature check, photo identification, etc. In fact, it is almost impossible to perform any of the physical world checks necessary to detect who is at the other end of the transaction. This makes the internet attractive to make one to commit fraud. According to a recent survey, the rate at which Internet fraud occurs is 12 to 15 times higher than physical world fraud (Tej Paul Bhatla, 2003).

2.7.1 Lost/ Stolen Cards

When one person looses his card or a card is stolen by some one or when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. This the easiest way for the fraudsters where he gets the information of the cardholders with out investing any on the modern technology. It is perhaps the hardest form of traditional credit card fraud to tackle.

2.7.2 Account Takeover

This type of fraud occurs when the valid customer's personal information is taken by the fraudsters. The fraudster takes control of a legitimate account by either providing the customers account number or the card number. The fraudster then contacts the card issuer, as the genuine cardholder, to ask the mail to redirect to a new address. The fraudster reports card lost and asks for a replacement to be sent. (Tej Paul Bhatla, 2003)

2.7.3 Cardholder-Not-Present (CNP)

CNP transactions are performed only on the internet that is remotely, in such kind of frauds neither the card nor the cardholder is present at the point-of-sale. This take many types of transactions such as orders made over the phone or Internet, by mail order or fax. In such transactions, retailers are unable to physically check the card or the identity of the cardholder, which makes the user unknown and able to disguise their true identity. The details of the credit card are normally copied without the cardholder's knowledge, collected from the receipts thrown by the customer or obtained by skimming process. Fraudulently obtained card details are generally used with fabricated personal details to make fraudulent CNP purchases. This means that while the three or four digit Card Security Code on the back of cards can help prevent fraud where card details have been obtained, but when the card is stolen it won't be helpful. (Tej Paul Bhatla, 2003)

2.7.4 Fake and Counterfeit Cards

This is another type of fraud where the creation of counterfeit cards, together with lost or stolen cards poses highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. The below mentioned are some of the techniques used for creating false and counterfeit cards: (Tej Paul Bhatla, 2003)

Erasing the magnetic strip

This is the type of the fraud where the fraudsters erase the magnetic stripe by using the powerful electro-magnet. The fraudster then tampers with the details on the card so that they match the details of a valid card, which they may have attained, for example, when the fraudster begins to use the card, the cashier will swipe the card through the terminal several times, before realizing that the metallic strip does not work. The cashier will then proceed to manually input the card details into the terminal. This kind of fraud is having high risk because the cashier will be looking at the card closely to read the numbers.
(Tej Paul Bhatla, 2003)

Creating a fake card

Today we have sophisticated machines where one can create a fake card from using the scratch. This is the common fraud though fake cards require a lot of effort and skill to produce it. Modern cards are having many security features, all designed to make it difficult for fraudsters to make good quality fraudulent. After introducing the Holograms in the credit cards it makes very difficult to forge them effectively. (Tej Paul Bhatla, 2003)

2.7.5 Skimming

Skimming is fast emerging as the most popular form of credit card fraud. Most cases of counterfeit fraud involve skimming. It is a process where the actual data on a card's magnetic stripe is electronically copied onto another. Fraudsters have been found to carry pocket skimming devices, a battery-operated electronic magnetic stripe reader, with which they swipe customer's cards to get hold of customer's card details. The fraudster does this whilst the customer is waiting for the transaction to be validated through the card terminal. The card holder doesn't know about this and it is very difficult for him to identify. In other cases, the details obtained by skimming are used to carry out fraudulent card-not-present transactions by fraudsters. Until the cardholder gets the bill to he don't understand what's the thing happened. (Tej Paul Bhatla, 2003)

2.7.6 White plastic

A white plastic is a card-size piece of plastic, same like a credit card of any color that a fraudster creates and encodes with legitimate magnetic stripe data for illegal transactions. The fraudsters use this at POS terminals for this they don't require card validation or verification. They mostly use this at the petrol pumps and at the ATMs where there will be no cashier working at the counter.

2.8 FRAUD TECHNIQUES

There are many ways in which fraudsters execute a credit card fraud. As technology changes, so do the technology of fraudsters, and thus the way in which they go about carrying out fraudulent activities. Frauds can be broadly classified into three categories, i.e., traditional card related frauds, merchant related frauds and Internet frauds. The different types of methods for committing credit card frauds are described below.
(Tej Paul Bhatla, 2003)

2.8.1 Merchant Related Frauds

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:
(Tej Paul Bhatla, 2003)

Merchant Collusion
This type of fraud occurs when merchant owners or their employees conspire to commit fraud using the cardholder accounts or by using the personal information. They pass on the information about cardholders to fraudsters.

Triangulation
Triangulation is a type of fraud which is done and operates from a web site. The products or goods are offered at heavily discounted rates and are also shipped before payment. The customer while browse the site and if he likes the product he place the online information such as name, address and valid credit card details to the site. When the fraudsters receive these details, they order goods from a legitimate site using stolen credit card details. The fraudsters then by using the credit card information purchase the products. This process is designed to cause a great deal of initial confusion, and the fraudulent internet company in this manner can operate long enough to accumulate vast amount of goods purchased with stolen credit card numbers.

2.8.2 Internet Related Frauds

The internet is the base for the fraudsters to make the frauds in the simply and the easiest way. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border, economic and political spaces, the internet has become a new worlds market, capturing consumers from most countries around the world. The below described are most commonly used techniques in Internet fraud: (Tej Paul Bhatla, 2003)

1. Site cloning:
Site cloning is where fraudsters close an entire site or just the pages from which the customer made a purchase. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are identical to those of the real site. The cloned site will receive these details and send the customer a receipt of the transaction through the email just as the real company would do. The consumer suspects nothing, while the fraudsters have all the details they need to commit credit card fraud. (Tej Paul Bhatla, 2003)

2. False merchant sites:
Some sites often offer a cheap service for the customers. That site requests the customer to fill his complete details such as name and address to access the webpage where the customer gets his required products. Many of these sites claim to be free, but require a valid credit card number to verify an individual's age. These kinds of sites in this way collect as many as credit card details. The sites themselves never charge individuals for the services they provide. The sites are usually part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudsters.

3. Credit card generators:

These are the computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. This makes the user to allow to illegally generating as many numbers as he desires, in the form of any of the credit card formats. (Tej Paul Bhatla, 2003)

The picture of general hacking of credit card (John G.Faughnan)

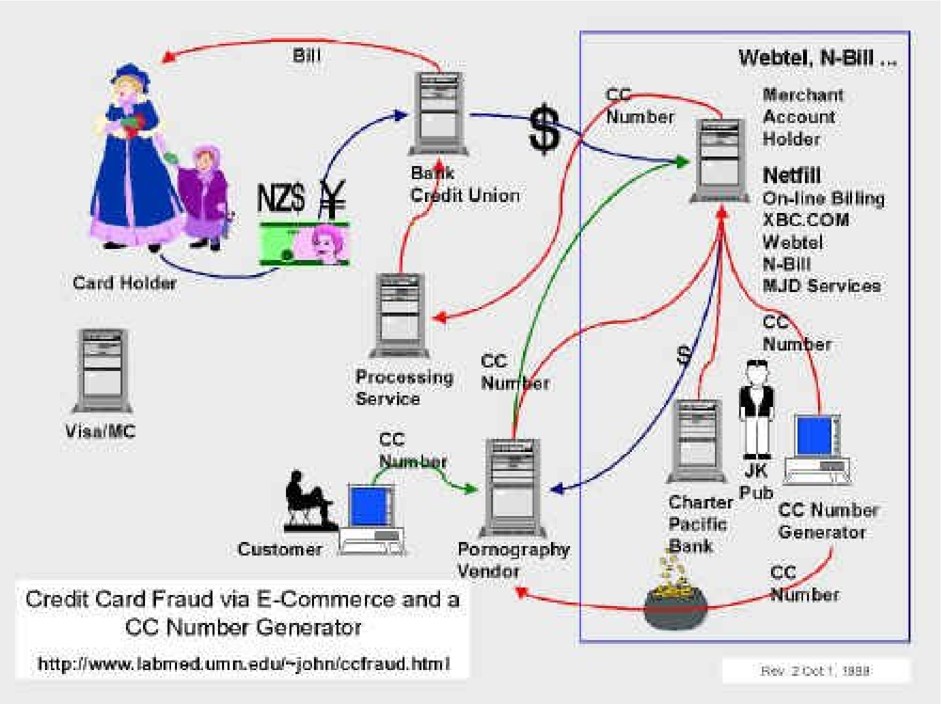


Fig-2.3 (International Net-Based Credit Card, by John G. Faughman, 2004)

Authentication

There are three basic methods for determining whether your credit card will pay for what you're charging: (http://money.howstuffworks.com/credit-card4.htm)

- Merchants with few transactions each month do voice authentication using a touch-tone phone.
- Electronic data capture (EDC) magstripe-card swipe terminals are becoming more common. Before checking out all should have to swipe their card in the terminal.
- Virtual terminals on the Internet

After the customer or the cashier swipes the credit card through a reader, the EDC software at the point-of-sale (POS) terminal dials a stored telephone number (using a modem) to call an acquirer. An acquirer is an organization that collects credit-authentication requests from merchants and provides the merchants with a payment guarantee.

When the acquirer company gets the credit-card authentication request, it checks the transaction for validity and the record on the magstripe for:

- Merchant ID
- Valid card number
- Expiration date
- Credit-card limit
- Card usage

In this system, the cardholder enters a personal identification number (PIN) using a keypad. The PIN is not on the card. That is encrypted in the cards database. (For example when we get cash from an ATM, that machine encrypts the PIN and sends it to the database to see if there is a match.) The PIN can be either in the bank's computers in an encrypted form or encrypted on the card itself. This type of cryptography where the transformation is used is called one-way. This means that it's easy to compute a cipher given the bank's key and the customer's PIN, but not computationally feasible to obtain the plain-text PIN from the cipher, even if the key is known. This was designed to protect the cardholder from being impersonated by someone who has access to the bank's computer files.

2.9 Theoretical framework

For further research we have adopted a Four-Factor theoretical frame work based up on which we proceed our work. The theoretical frame for this master thesis would be underpinned by the theory put forward by Chris Brenton, (2003), according whom in his Article of "Mastering Network Security" he uses the theory of Daniel Buttafogo and Larry Drexler, Who says that "Detection is considered in two perspectives, from the Point-Of-Sale (POS) and the Internet".

➢ *Application process.*

The application process represents the first line of risk management defense. (Arata Michael J., 2004). It is common practice for card issuers to confirm an applicant's information through multiple data sources. The issuer of the credit card makes a call to the customer's phone number which is mentioned on the application form, he further check the address for verification. Certain high-risk applications may be pulled for a detailed review depending upon the channel used, the applicant's geographic location or other special characteristics. Unsolicited applications from the Internet channel are almost always reviewed given the authentication problems described above. Applications may also be pulled for review when received from geographic areas where high incidences of credit card fraud have been reported in the past.(Wolfgang Rankl.and Wolfgang Effing, 2004). Applications are also tested for inconsistencies with information received from credit bureaus. These might typically include names, addresses or phone numbers that do not match and might signal an attempt to create a fraudulent account. (Peter Burns, 2002)

According to Arata 2004, frauds such Identity theft and CPN could be addressed when much attention is paid and resources deployed to build effective systems at the application process level. Wolfgang R, 2003 intimated that the application process must be well veted which could help prevent identity theft.

- ***Activation process.***

Issuers also build in fraud controls when a new card is activated by the customer. When calling to activate the card a flag may be raised if the call does not originate from the home phone number listed on the application. In such circumstances, rather than automatically activating the account, the caller is transferred to a customer service representative who will attempt to verify the caller's identity using other information from the application or information obtained from the credit bureaus. (Peter Burns, 2002)

The activation process provides a platform to check the caller's details with that of the card holder. According to Cristian Radu, 2003, at this level, the identity of the person in possession of the new card is established and where it differs from information received from the application process, the activation could be put on hold or stopped for further investigation. Activation process is used to prevent frauds such as identity theft, CPN, account takeover or fake and counterfeit cards (The Silver Lake 2002)

- ***Transaction behavior monitoring.***

Sophisticated card issuers monitor high-risk situations and transactions in a proactive attempt to prevent fraudulent transactions. Examples of high-risk situations that may receive special monitoring would include the opening of new accounts and the sudden and intense usage of cash advances. Sophisticated neural network software is commonly used to monitor transaction behavior to flag unusual activity. For example, a series of cash advances by a cardholder who rarely uses his card for cash advances may trigger an investigation and perhaps a call to the cardholder to verify these cash transactions. Similarly, large dollar purchases at a location far removed from the cardholder's normal purchasing area might similarly be flagged for further investigation and verification. All such high-risk activity and transactions are typically reviewed against files of known lost or stolen cards. (Peter Burns, 2002)

All types of frauds predominantly occur and are identified during and after transactions. The transaction behavior monitoring process could therefore prevent almost all identifiable frauds after effective tracking albeit, it may take longer periods. It is quite difficult however to detect first time frauds using the transaction behavior monitoring process which requires tracking of transactions emanating from the credit card source. Wolfgang R, 2003)

- ***Detection & Fraud Prevention on the Internet***

The Internet and the anonymity associated with card not present transactions present unique fraud management challenges. Authentication of the cardholder is a fundamental requirement in managing fraud on the Internet and there are no universally accepted solutions. As a result, credit card fraud on the Internet is substantially greater than in the physical, or even, phone environments. (Peter Burns, 2002)

One approach to combat Internet fraud, which is supported by many issuers, is Card Verification Value 2 (CVV2). The set of three digits found on the reverse side of most credit cards is unique to that card. Merchants that require Internet customers to enter this value along with the actual card number, add a layer of security to the transaction. Since the three-digit value can only be found on the card itself, there is a greater likelihood that the purchaser is actually in possession of the card. Stolen charge receipts, for example, would not reveal the card's three-digit card verification value. However, if the card being used has been stolen, this is obviously not an effective preventive measure (Cristian Radu, 2003)

The use of account number masking software is another new method being employed as a way to control Internet fraud. The key element of this process is a single use number for each transaction. A handful of issuers have unveiled programs that add this extra step to the online shopping process. Generally, after the consumer has selected their items for purchase from an e-tailer and is ready to check out, then they log on to their card issuer's web site. On the web site they select the card they wish to use to pay for the purchase. At this point a unique credit card number and expiration date is created and used to finish the online purchase. It has been suggested that consumers are unwilling to accept the inconvenience associated with the added steps. Other observers suggest that consumers simply are not that concerned about using credit cards on the Internet. David S. Evans and Richard Schmalensee, 2003 emphasized that an important underlying factor in the dealing with fraud on the Internet is that, rather than issuing banks or consumers are responsible for most of the financial cost of card-not-present fraud.

Although lost or stolen cards frauds can hardly be prevented by the introduction of the CVV2, it has so far been proven successfully in handling CPN, account takeover, skimming and fake and counterfeit card frauds (Arata Michael J., 2004).

3.0 METHODOLOGY

In this Chapter, we describe the methods used for conducting our Research Process. Initially we describe the Research Methodology and then Research Process. Finally we describe our Research Method and attempt to justify the basis for the selection of the method.

3.1 RESEARCH METHODOLOGY

According to Macleod Clark "... An attempt to increase the sum of what is known, usually referred to as 'a body of knowledge', by the discovery of new facts or relationships through a process of systematic inquiry, the research process". *(John Ross, 1999)*

3.2 RESEARCH PROCESS

According to Geoff Lancaster Marketing research is a planned formal approach to the collection of marketing information and it has a number of distinct stages.

3.2.1 Problem definition

It is leading to a preliminary statement of research objectives to provide information, making this stage an identification of information needs which are: Motivations, values, beliefs, feelings, opinions, evaluations, attitudes, intention knowledge, facts, behavior, actions , demographic, socio-economic etc. This information is required for exploration, description, prediction or evaluation. It comes from Secondary data sources, both internal and external to a company Primary data sources. (Geoff Lancaster, 1990)

3.2.2 Review of secondary data sources

Such as company records, reports, previous research trade associations, government agencies, research organizations advertising/market research agencies, books, periodicals, theses, statistics, conference proceedings, etc. (Geoff Lancaster, 1990)

3.2.3 Select the research approach for collection of new/primary information

Through a combination of:-

- Experimentation
- Observation
- Surveys - mail, telephone, personal
- Motivational research techniques - depth interviewing, group interviewing, Projective techniques

3.2.4 Research design

Creating an effective research design is likely to be one of the most difficult and eminently useful tasks in drafting a proposal. An effective research design links abstract and stylized concepts and questions with the empirical world's complexities and challenges. A research design must at once be specific and highly flexible. It must be expansive enough to adapt these very complexities while still pointing you towards relevant data.

3.2.5 Data collection

According to Yin, there are six different ways to collect data for case studies. These include; documentation, archival records, interviews, directs observations, participant observation, and physical artifacts. The primary source of method used for collecting the data is Interview method. (Yin, 2002)

Interviews appear to be the more reliable source of case study information. These interviews are important because they are target oriented and focus directly on the research topic giving a deeper insight into a topic. (Yin, 2002)

During the creation of questionnaires, we will try to avoid questions that only give yes or no answers. We believe that by doing this we will obtain factual data, which are more centered, and relevant to the questions, even though it was a yes or no question.

Besides the interviews, we will use other sources to capture data. Paramount of these shall be literature from the journals and electronic databases in the library of Lulea University of Technology and other science related databases such as EMERALD, Science direct, etc.

3.2.6 Analysis and Interpretation of data

The most important thing to know about data is that it has to be interpreted. It is about an approach that was first developed in 1960s by two American sociologists. They claim that data collection and data analysis taking place in close conjunction, and feeding into each other. They bring up three phases of data collection and analysis taking place in close conjunction, and feeding into each other. They bring up three phases of data collection and analysis. Open coding that is the preliminary phase of analysis, axial coding that is seeking of the connections between the categories identified and finally the theoretical coding that is the evolution of a paradigm and a conditional matrix.

In our thesis, we shall first conduct a preliminary analysis from the interviews. Secondly, we would try to see if there were any connections between the interviewees' answers and how those connections could be explained. We would further try to simplify and prune the data in other to obtain a rather easy to understand data. Finally, we shall compare our analysis with the theory to and thereupon draw our conclusions.

3.3 RESEARCH APPRAOCH

Research methods can be classified in various ways; however one of the most common distinctions is between qualitative and quantitative research methods. (Michael D. Myers, 2002)

3.3.1 Quantitative Research Methods

Quantitative Research Methods were originally developed in the natural sciences to study natural phenomena. Examples of quantitative methods now well accepted in the social sciences include survey methods, laboratory experiments, formal methods and numerical methods such as mathematical modeling. Qualitative data sources include observation and participant observation, interviews and questionnaires, documents and texts, and the researcher's impressions and reactions. (Michael D. Myers, 2002)

According to Guba and Lincoln, suggest four underlying paradigms for qualitative research: positivism, post-positivism, critical theory, and constructivism**.** Suggest three categories, based on the underlying research epistemology: positivist, interpretive and critical.

There are three basic research paradigms -- positivism (quantitative, scientific approach), interpretivism, and critical science. (Michael D. Myers, 2002)

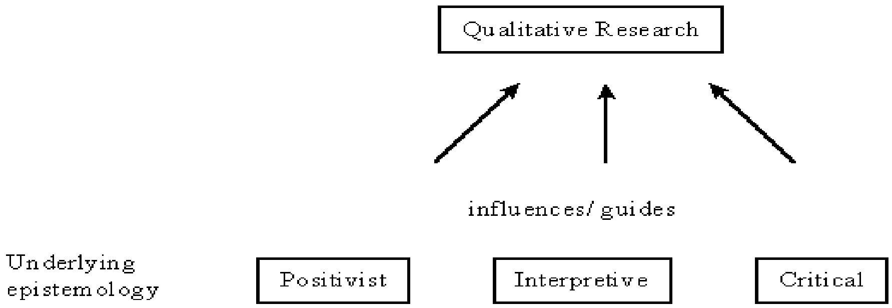


Figure 1. Underlying philosophical assumptions

Fig-3.1 (Qualitative Research in Information Systems, by Michael D. Myers, 2002)

Positivist Research

Positivists generally assume that reality is objectively given and can be described by measurable properties which are independent of the observer and his or her instruments. Positivist studies generally attempt to test theory, in an attempt to increase the predictive understanding of phenomena. In line with this classified IS research as positivist if there was evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from the sample to a stated population. (Michael D. Myers, 2002)

Interpretive Research

Interpretive researchers start out with the assumption that access to reality is only through social constructions such as language, consciousness and shared meanings. The philosophical base of interpretive research is hermeneutics and phenomenology. (Michael D. Myers, 2002)

Critical Research

Critical researchers assume that social reality is historically constituted and that it is produced and reproduced by people. Although people can consciously act to change their social and economic circumstances, critical researchers recognize that their ability to do so is constrained by various forms of social, cultural and political domination. The main task of critical research is seen as being one of social critique, whereby the restrictive and alienating conditions of the status quo are brought to light. Critical research focuses on the oppositions, conflicts and contradictions in contemporary society, and seeks to be emancipatory i.e. it should help to eliminate the causes of alienation and domination. (Michael D. Myers, 2002)

3.3.2 Qualitative Research Methods

There are various qualitative research methods. The four research methods that will be discussed here are action research, case study research, ethnography and grounded theory. (Michael D. Myers, 2002)

Action Research

Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework.

Case Study Research

Case study research is the most common qualitative method used in information systems. Although there are numerous definitions, according to Yin, defines the scope of a case study as follows:

A case study is an empirical inquiry that:

Investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.

(Michael D. Myers, 2002)

Ethnography

Ethnographic research comes from the discipline of social and cultural anthropology where an ethnographer is required to spend a significant amount of time in the field. Ethnographers immerse themselves in the lives of the people they study and seek to place the phenomena studied in their social and cultural context.

Grounded Theory

Grounded theory is a research method that seeks to develop theory that is grounded in data systematically gathered and analyzed. According to Martin and Turner (1986) grounded theory is "an inductive, theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data. (Michael D. Myers, 2002)

Qualitative versus Quantitative Research: (James Neill, 2004)

Features of Qualitative and Quantitative Approach

Qualitative	***Quantitative***
"All research ultimately has a qualitative grounding" - Donald Campbell	"There's no such thing as qualitative data. Everything is either 1 or 0" - Fred Kerlinger
The aim of ***qualitative*** analysis is a complete, detailed description.	In ***quantitative*** research we classify features, count them, and construct statistical models in an attempt to explain what is observed.
Recommended during earlier phases of research projects.	Recommended during latter phases of research projects.
Researcher may only know roughly in advance what he/she is looking for.	Researcher knows clearly in advance what he/she is looking for.
The design emerges as the study unfolds.	All aspects of the study are carefully designed before data is collected.
Researcher is the data-gathering instrument.	Researcher uses tools, such as questionnaires or equipment to collect numerical data.
Data is in the form of words, pictures or objects.	Data is in the form of numbers and statistics.
Qualitative data is more 'rich', time consuming, and less able to be generalized.	Quantitative data is more efficient, able to test hypotheses, but may miss contextual detail.
Researcher tends to become subjectively immersed in the subject matter.	Researcher tends to remain objectively separated from the subject matter.

Table 3.1. Features of Qualitative and Quantitative Approach

3.4 OUR APPROACH

As we discussed all the different Qualitative and Quantitative Research Methods, Our research study is the case study and we feel that Survey Method of Qualitative Research suits best for getting better results. This approach is characterized by flexibility, which makes it possible to change the study by adding questions and changing the order. Moreover the purpose has also been to gain in-depth knowledge in the problem area by creating understanding through the interpretation of the theory.

Our main Concept is How to stop the Hacking of Credit Card Details in the Internet arena, which is a very complex concept, which has to be decreased to the maximum extent. We therefore felt that Qualitative Approach and the Case study using the Survey Technique Method is the best suitable method for our study because survey is a non-experimental, descriptive research method.

CASE STUDY

A case study protocol contains more than the survey instrument, it should also contain procedures and few rules that to be follow. That is to be created before the data collection phase. According to Yen, presented the protocol as a major component in asserting the reliability of the case study research. A typical protocol should contain the following sections. (Winston Tellis, 1997)

- An overview of case study project
- With in case analysis
- Cross case analysis.

An overview of the case study in our thesis is we choose two cases. Our two cases are the FSB Bank in Sweden and Andhra Bank in India. Our main focus as already discussed in chapter one will only to be proving the effect of advanced techniques used by banks in advanced countries, in our case SWEDEN, when compared to developing countries (Which here is INDIA).

For the data collection part in our case study we use survey technique. We used this technique because this is best suited to our type of approach. As our research is to investigate difference of techniques in banks, survey method is best.

Survey Research Method

The survey is a non-experimental, descriptive research method. Surveys can be useful when a researcher wants to collect data on phenomena that cannot be directly observed. Surveys are used extensively in library and information science to assess attitudes and characteristics of a wide range of subjects, from the quality of user-system interfaces to library user reading habits. (Basha, 1980)

In our survey research method we did data collection using the interview mode. We collect data from the two banks. We use these two modes of survey for our convenience as we choose two case studies.

Modes of survey

- Personal (Face-to-Face)
- Telephone

Personal Interviewing

Personal Interviewing generally yields highest cooperation and lowest refusal rates. It also allows for longer, more complex interviews. The response we get here is very high quality. With Personal Interviews we can have the presence of interviewee so that we can get more information from him and his response can be viewed. (Linda K. Owens, 2002)

From the swedish bank we collect data by conducting personal interviewing with the employee in the bank. To know the techniques they are using in their bank.

Telephonic Interview

Telephonic interview is the method, which is very less expensive than personal interviews. Here we take RDD samples of general population for interviews in telephone. Here we get better response then from the mail for list samples. We can also have a better control and supervision of interviewers. (Linda K. Owens, 2002)

We use this mode of data collection for the bank in india, we take interviews from the employes and the customers in that bank who faced the problems in the use of credit card.

WITHIN CASE ANALYSIS

After we collected the data from the case sites, we then analyse the two case site empirical data with the four factors of the theoretical frmae wok.

CROSSCASE ANALYSIS

This is the next step after the analysis and this is the final step used to analyze the empirical data from the case sites. After we evaluating the similarities from the both banks, we then cross case that with the four factors which we used in the theoretical frame work.

3.5 REALIABILITY AND VALIDITY

‘Reliability’ is a concept, which used to test or evaluate qualitative research. The idea is most often used in all kinds of research. If we see the idea of testing as a way of information elicitation then the most important test of any qualitative study is its quality.

A good qualitative study can help us to understand a situation that would otherwise be confusing”. According to Stenbacka, (2001) “the concept of reliability is misleading in qualitative research. If a qualitative study is discussed with reliability as a criterion, the consequence is rather that the study is no good” (Nahid Golafshani, 2003)

On the other hand, Patton (2001) states that validity and reliability are two factors, which any qualitative researcher should be concerned about while designing a study, analysing results and judging the quality of the study. This corresponds to the question that “How can an inquirer persuade his or her audiences that the research findings of an inquiry are worth paying attention to?". To answer to the question, Healy and Perry (2000) assert that the quality of a study in each paradigm should be judged by its own paradigm's terms. (Nahid Golafshani, 2003)

To ensure reliability in qualitative research, examination of trustworthiness is crucial. Seale (1999), while establishing good quality studies through reliability and validity in qualitative research, states that the “trustworthiness of a research report lies at the heart of issues conventionally discussed as validity and reliability”. When judging qualitative work, (Strauss and Corbin, 1990) suggest that the "usual canons of ‘good science’…require redefinition in order to fit the realities of qualitative research"

The concept of validity is described by a wide range of terms in qualitative studies. This concept is not a single, fixed or universal concept, but “rather a contingent construct, inescapably grounded in the processes and intentions of particular research methodologies and projects”.

In order to increase the validity we have critically examined both the theoretical and the empirical materials to ascertain their relevance to our research question and the problem area. Further more we relied on authoritative books and research materials to enhance the validity. In most situations we have used original sources for our secondary data. We have tired to increase validity by using sources that are reliable as much as possible.

4.0 EMPIRICAL DATA

This Chapter, we present the data from the two banks, one from India and another in Sweden. The research findings from our study are illustrated in this.

In this study we have chosen the respondents from the bank in India that are issuing the credit cards, as we find it is more important in order to get interviews as possible, from the respondent's point of view. We have chosen to interview banks who are issuing credit card. Both the bank employees who are working in credit card issuing department and the customers in that bank.

In this chapter, the answers from the interviews are presented. The Banks information is also briefly presented. The employee or the customers are not mentioned by name, instead they have represented with some number.

Two financial institutions, Andra Bank located in Hyderabad in India and the other Foreningssparbanken AB, Luleå branch in Sweden were selected as the primary source for the collection of our empirical data. These two institutions could be classified as a single industry considering the products and services they provide. According to Kurhana (1999), the single industry studies are more excellent for exploratory research due to the fact that they reduce or even eliminate the complexity that comes from cross industry variability.

4.1 CASE SITE 1: ANDHRA BANK, INDIA

Background of Andhra Bank

Andhra Bank was founded by Dr.Bhogaraju Pattabhi Sitaramayya. The Bank was registered on 20th November 1923 and commenced business on 28th November 1923.

Andhra Bank is the first Bank to issue Credit Cards in India since 1981. The Bank issues four types of cards namely - Visa Classic, Visa Gold, Master Card and Master Card Electronic. All these cards are accepted in India and Nepal at Merchant establishments which display VISA / Master card acceptance symbol. Further VISA Gold cards are accepted at 50 000 visa merchant outlets and millions worldwide.

Cash drawing facility against credit cards is extended at 110 branches of Andhra Bank and also at other Bank branches equipped with EDC's and ATM's of Andhra Bank. These cards are also accepted at other Bank ATM's displaying VISA/MasterCard acceptance symbol. Credit Card Department has exclusive card centers at 19 important cities to extend service to the cardholders. All the branches entertain applications for new Credit Cards.

Respondent No. 1:

According a respondent, a Manager in Andra bank from past 4years, they are good at providing the best services in Baking especially in Credit Card department. They have thousands of customers using credit cards. There are some problems registered about credit card frauds. Online purchasing is the most critical area where the credit card fraud occurs. They have most of the complaints because of online stores only. Now-a-days using a credit card in Online stores is very dangerous because there are many problems arising like credit card details theft, inappropriate usage, problems with hackers, etc… they said they are in dilemma whom to believe and whom not, because every one says that they are ***RISK FREE ONLINE STORES***. There are many companies using the website that looks similar to another trusted website and encourage the customer to enter the details of Credit Card. After getting details of credit card they close their website. This is all happening over Internet. He said it's quite difficult to stop these issues. He further stated that the bank employees are working for eighteen hours to the customers, except night six hours. He said the people should be very careful while purchasing a product in Online Store. In their bank they have registered cases like this and this is mainly because of using their credit card in Online Stores. So, the bank authority are planning to introduce a new authentication method which gives more secure to the credit card customers and prevent them from hackers. He said they are working on that process and once it is completed they will release a Newsletter of it and protect the customers.

Respondent no. 2:

According to him, he is the Employee working in credit card department since 3 years. There are some different kinds of problems registered with him. Most of the cases are Credit Card frauds over the Internet. He used to get these complaints now and then. '*Here the most reliable security measure in place is through the PIN authentication. In this wise, clients and customers are always advised never to expose their PIN to any other person' he stated:*

He further stated that most of the preventive measures can emanate from the customers side. They therefore educate their clients and send out information on the dangers in exposing ones card details and most especially the Personal Identification Number, PIN to another person. They are particularly concern about where and how customers use credit cards and the details to be given in Internet sites.

Here we are using the data collected from customer in order to support our problem area of concern of security. Here we have collected response of few potential customer being determined by the regular usage of the cards(and have highlighted the problem faced by them or to be précised the concern of security. Note this data would not be a part of our analysis as this is only used to support our problem area,

AB Customer 1:

"I have been using the Credit Card for the past 3 years. I never experience any problem both online or offline with my card until recently when I effected online payment at a website which happened to be a fraudulent site. After entering my card details, I later detected that an amount of 40,000rs had been withdrawn from my account. A quick cross check from my bank established that I've been duped", he stated.

AB Customer 2:

According to another respondent who happened to be a customer of the same bank, he has been using credit card for more than two years. He said a few weeks ago, he got a phone call from Office Max. They asked me to verify the delivery address for the new $2500 computer, which was ordered. He informed them that he had not ordered a new computer and asked them for the address to which it was supposed to be delivered. They mentioned his name and address exactly. He was shocked to listen this because he never ordered a computer. He has been using his credit card regularly for making online purchases. He realized that he has purchased a product from Office Max few months before. That product has been delivered to him in-time. They have used that same data for making fraud. They say that they have the proof that he orders the computer worth $2500. He has never ordered a computer but they made fraud and used his credit card details. He decided to give a complaint against them.

AB Customer 3:

According to the customer 3 of Andhra Bank using its credit card since 3 years. He would like to put out a serious warning for anyone considering the supposed 'credit' offer from a company called CMA. They are not only extremely unprofessional and deceptive, but quite rude about it as well. He received an email, actually it was 'spam', and something he usually delete right away. However, with the "enticement" of a guaranteed 2 or 3 credit cards, with no security deposit required, and he himself in need of a laptop for his web design. Now, in the email ad it very clearly states 'Risk Free', and invites to 'Apply Now'... So, thinking he had nothing to risk, he "applied", to see what would come up. He don't know at that point if he just 'missed' the 'catch' or if something was changed since he applied, but it appears that when filling out the application, he had legally bound himself to pay them the $1500. Not realizing this, he is innocently emailed them and told them that he was still considering their program, but how would he know that he wouldn't receive offers from 2 of the credit cards he already have? What he received back was an email telling me to make a payment on his account now or risk late fees. Totally befuddled and confused, he again, very innocently emailed back and said 'what payment? He hasn’t done this yet'... and the reply he received was the rudest, threatening, and harassing email that he think he have EVER received from a so-called company.

They stated to him that not only he was obligated to pay the $1500, but he was now going to be charged a $100 late payment fee, threatening that they "have his credit report" in their possession, as if holding it hostage almost. Now he was forced to pay the total sum to them.

AB Customer 4:

According to the customer 4, he is using the credit card since 2 years. He is just using his credit card details for purchasing products in online stores. He regularly makes purchases through Internet. One day all of a sudden he went to a merchant store to purchase few products. He knows that there is much amount in his Credit Card. He has chosen the products and he has given his Credit Card for Payment. Then the merchant has said that this card has no amount in it. He was really shocked to listen that. Then he made a call to the Bank to know the status. They said that there is no amount in the Card. Some one has hacked his credit card details and used his money. As he uses his credit card daily he doesn't know where the mistake has happened. He doesn't know which online store has made fraud to him. He was very confused. He had gone to bank to have all the clear details. Every thing is correct but 3 days back 1, 00,000rs have gone from his account. He didn't make that transaction. He lodged a complaint on it.

AB Customer 5:

According to the customer of Andhra Bank, she has been using Credit Card since 2 years. One day, Andhra Bank refused to accept her charges and insisted that they had supplied a product that she asked for. She in turn asked them "How did you manage to forge my signature?" She received copy of the application form allegedly filled by her. To her horror, the application form bore a signature, which carried absolutely no resemblance to her signature. In simple words, it was a fake signature and a fake handwriting. A different form was filled without her consent and her signature was conveniently forged. Even her Form 16 was signed with forged signature. She dashed an email to Andhra Bank Credit Cards – Head of Customer Service Quality

In these circumstances, she is determined to bring Andhra Bank's fraudulent tactics to a public forum. She is in process of drafting a complaint letter to The Reserve Bank of India, with a CC to Newspapers (Times of India, Economic Times, Indian Express, Maharashtra Times, Lokasatta, Hindustan Times, Mid day, etc.)

4.2 CASE SITE 2: FORENINGSSPARBANKEN AB, Luleå

Background of FSB

There are two basic online banking facilities that foreningssparbanken (FSB) AB operates, apart from the normal bankcards that they issue to their clients. These are the Online banking service and the e-card service. Securities in both services are very crucial to them as financial institution.

Security in Internet Banking

The Internet banking is just the extension of the normal or traditional banking services or practices onto the Internet. With the online or Internet banking, customers are able to log on and transact banking businesses from everywhere and anytime. These therefore make it imperative for the banks to institute high security measures.

The security system in our online banking service consists of several elements in order to provide maximum security. The digital bank vaults around our data systems are called firewalls. The connection between your computer and our web servers is encrypted, which means that no one else can see the information sent between you and the bank. We assign an electronic device called The Personal Security Authenticator (PSA) to the customer. The PSA with the individual's code is another means of preventing anyone else logging in the place of the customer. If the customer logged in but have not used the service for the last 15 minutes, a dialogue box will appear on the screen, asking whether you wish to continue. This is to prevent an unauthorized person from getting access to your account in case of any eventuality.

- *Online Banking Security Administrator (FSB, Luleå)*

As to how the bank test or upgrade their security solutions since fraudsters are always prowling around to find means of breaking into systems, the Administrator at FSB stated:

"We keep up-to-date with the development of security solutions in order to maintain the highest level of security. We always caution our customers and clients to remember that their security authenticator is an identification document and should be kept in a safe place.

When one logs in using a personal code, for security reasons, she cannot always carry out all bank transactions. For instance, she cannot carry out transactions involving transferring money from her own finances, e.g. paying bills or transferring money to anyone else's account".

Implementing effective security measures is identified as a responsibility of both the bank and the customers. Where as the bank ought to put in place effective checks and control as well as high network intrusion detection security mechanisms, the customers are responsible for ensuring that Internet traffic is as secure as possible.

Security in e-card

E-card is a service that you link to your ordinary bank, debit and credit cards. You can then pay safe and easy by card on the Internet without giving out your real card number. E-card generates a unique card number each time you need to make a payment. You need a personal code to use e-card. This is the same as when you log in without a security authenticator.

The security authenticator and its functions are based on the security system that safeguards our online banking service. It serves as your ID card and gives you new codes (passwords) each time you log in or sign a bank transaction.

The e-card is administered by the Swedbank for banks located in the country.

E-card from the Swedbank is the safe, effective and easy way for cardholders to shop online, without ever transmitting their actual credit/debit card details over the Internet. By using an e-card, the cardholder can eliminate the risks of card fraud and identity theft that result in credit card numbers being exposed and potentially compromised.

Using the Swedbank's online banking website, the e-card service means that the cardholder can generate unique numbers linked to the cardholder's actual card account. These e-cards are complete with expiry date and signature panel code (CVV2/CVC2), and can be used in place of real credit or debit card details while shopping online.

The major card schemes Visa and MasterCard, do not distinguish between an e-card and a "real card" number. E-card payments are authorized and settled in the very same way as 'real card' payments. The merchant receives their payment and the cardholder receive their goods and services, while their real credit / debit card details are never transmitted over the Internet.

At the client level, adequate measures are put in place to encourage and also tighten the security. A respondent echoed that;

Cardholder's can also apply extra controls to their e-card. For example, a cardholder may limit the value of each transaction, determine when the e-card will expire, restrict an e-card for use at a single merchant, and even limit the total amount spent on a single e-card. E-cards from Swedbank can be used for a single purchase at a specific merchant, or for a recurring charge such as a subscription service. Additionally, a cardholder can generate an e-card that can be registered at a merchant's site, for continued use only at that merchant.

According to a risk management expect at the bank, her role in managing fraud control efforts at the bank broadly characterizes this risk management role in the industry, "My objective is to make fraud difficult to commit, detect it quickly when it does occur, stop it as soon as possible and learn how to better protect the bank in the future."

5.0 DISCUSSION AND ANALYSIS

In this Chapter, to answer the main question we link the theory and empirical findings through analysis and discussions. We proceed further by cross analyzing with the factors of theoretical frame work.

INTRODUCTION:

In this section we present the analysis and discussion from our empirical findings as outlined in the previous chapter. Our analysis would be considered from two perspectives. First we look at that two case studies and perform a within case analysis and there after conduct a cross case analysis on the two case sites, where we would attempt to find out the similarities and differences between our two cases. This discussion and analysis is based on the four critical detections and risks management methods or practices as presented by Buttfago and Dyxler in the theory presented in chapter two. These practices are:

- Application process
- Activation process
- Transaction behavior monitoring
- Fraud prevention on the Internet

5.1 WITHIN CASE ANALYSIS

The within case analysis is the first of the two phases in analyzing the empirical data we obtained from the case sites. These also include the outcome of the discussions we undertook on the data.

5.1.1 Case Site 2: Andhra Bank, India

The Andhra Bank, like many other banks worldwide view security and security threats as a high priority in their operations. From management to the from desk clerk, all pursue the banks policy on offering free security information as well as education and tit bits on how to secure their accounts and most especially online card users from fraudsters.

Application Process

At the Andhra Bank the application process represents the first line of risk management defense. An applicant's information is normally confirmed through a single source, usually the forms that the applicant complete when first seeking for the bank's service. The banks also do phone address to determine if the phone number on the application matches the address as defined by the area code on the application. However high-risk applications are not review in detailed depending upon the channel used, the applicant's geographic location or other special characteristics. Another area the Andhra bank seems to be doing little is the review of unsolicited applications from the Internet channel. Applications are also seldom tested for inconsistencies with information received from other credit bureaus. According to the theory however, these might typically have data that do not match and might signal an attempt to create a fraudulent account.

Activation Process.

The Andhra bank activation processes include the building of fraud controls when a new card is activated by the customer. Here there is no automated check on the phone number but it requires a bank staff to receive the call and manually check on the cardholder's details at the bank. This however places some time limitation on the use of the card. Between 23:00pm and 05:00 there is no bank official in attendance to pick such calls for verification and authentication.

Transaction behavior monitoring.

Andhra bank by the current status cannot be described as a sophisticated card issuer. Solution to the monitoring high-risk situations and transactions in a proactive attempt to prevent fraudulent transactions are yet to meet by the bank. Here anytime cardholder reports of a missing card or a suspected fraudulent move, the bank immediately place a temporal suspension on the cardholder's account. The balance in the account is transferred to suspense but a mechanism is established to allow the account owner withdraws or undertake other banking transactions except the payment or withdrawal by the lost credit or online card. The bank keeps record on individual complains and all such high-risk activity and transactions are typically reviewed against files of the known lost or stolen cards. We believe is not a good method for fighting fraud. These records are of little importance to the cardholder when it comes to fraud prevention.

Fraud prevention on the Internet

Preventing Internet fraud continues to be one of the major hurdles confronting the Andhra bank. Credit card fraud on the Internet is substantially greater with bank than all others in the physical and phone environments combined. The credit card system in the Andhra bank does not support the Card Verification Value 2 (CVV2). The absence of the CVV2 which is currently viewed by many a security expects as one of the most effective means of combating credit card frauds in the internet leaves a huge gap in the bank's current approach of preventing fraud on the internet. In its place the bank uses the account number masking software which is rather a new method being employed as a way to control Internet fraud. Here the process involves a single use number for each transaction. Though this method has so far proven to be effective albeit, only about very few of the banks credit card clients (as at November, 2005), has so far adopted it.

5.1.2 Case Site 2: Foreningssparbanken AB, Luleå

Application process.

At the Foreningssparbanken AB (FSB), the application process forms part of the first line of risk management defense. Different online cards are issued by the bank or other card issue authorities on the behalf of the bank. Among the cards processed by the FSB are the MasterCard, Visa Card and the Maestro. The MasterCard and the Visa are issued by third parties thus MasterCard International and Visa Association whereas the bank issues the

Maestro that is mostly a debit card. At the FSB, both phone address and distance calculations are employed to determine if the phone number on the application matches the address as defined by the area code on the application. They also try to confirm an applicant's information through multiple data sources. Applications are often pulled for review when received from geographic areas where high incidences of credit card fraud have been reported in the past. FSB also tests applications for inconsistencies with information received from credit bureaus. These usually include names, addresses or phone numbers that do not match and might signal an attempt to create a fraudulent account.

Activation process.

When a new card is activated by the customer, FSB build in fraud controls. When calling to activate the card a flag is normally raised if the call does not originate from the home or registered phone number listed on the application. This system is also automated and thus automatically activates the account, where the caller's identity is verified. Alternatively, there is also in place an automatic transfer or redirection to a customer service representative who will attempt to verify caller's identity using other information from the application or information obtained from the credit bureaus.

Transaction behavior monitoring.

FSB monitor high-risk situations and transactions in a proactive attempt to prevent fraudulent transactions. High-risk situations such as the opening of new accounts and the sudden and intense usage of cash advances are given priority in monitoring their bid to combating credit card fraud. The bank has in place sophisticated neural network software which is used to monitor transaction behavior to flag unusual activity. For example, a series of cash advances by a cardholder who rarely uses his card for cash advances may trigger an investigation and perhaps a call to the cardholder to verify these cash transactions. Moreover, high-risk activity and transactions are typically reviewed against files of known lost or stolen cards.

Fraud prevention on the Internet

One major approach that has been successful in managing Internet payment frauds at the Foreningssparbanken is the adoption of the Verification Value 2 (CVV2). This is used to support the MasterCard and the Visa Cards for online transactions. The set of three digits found on the reverse side of most credit cards is unique to that card. Merchants that require Internet customers to enter this value along with the actual card number, add a layer of security to the transaction. Since the three-digit value can only be found on the card itself, there is a greater likelihood that the purchaser is actually in possession of the card. One good measure here is that stolen charge receipts, for example, would not reveal the card's three-digit card verification value. However, if the card being used has been stolen, this is obviously not an effective preventive measure.

Apart from this FSB also uses the e-card system in its Internet banking. With the e-card it is the safe, effective and easy for cardholders to shop online, without ever transmitting their actual credit/debit card details over the Internet. By using an e-card, the cardholder does eliminate the risks of card fraud and identity theft that result in credit card numbers being exposed and potentially compromised. The e-card service means that the cardholder can generate unique numbers linked to the cardholder's actual card account. These e-cards are complete with expiry date and signature panel code (CVV2/CVC2), and can be used in place of real credit or debit card details while shopping online. The other thing is that the major card schemes Visa and MasterCard, do not distinguish between an e-card and a "real card" number. E-card payments are authorized and settled in the very same way as 'real card' payments. This is equivalent to the account number masking.

Moreover there is the flexibility but high security control for cardholder's who can also apply extra controls to their e-card. A cardholder is offered the option of limiting the value of each transaction, determine when the e-card will expire, restrict an e-card for use at a single merchant, and even limit the total amount spent on a single e-card.

5.2 CROSS CASE ANALYSIS

The cross case analysis is the second and final step used to analyze the empirical data from our case sites. Here we look at the scenarios at two banks by evaluating the similarities and differences in their credit card fraud prevention approaches. Similar to the within case analysis considered above the four modalities outlined by Buttfago and Dyxler will form the theoretical underpinning of the analysis.

5.2.1 Analysis: Application Process

At Andhra, India and the Foreninssparbanken, Luleå banks, the application process serves as the first line of managing risk and defense. Both banks also use the phone method to determine the address matching in the authentication of a true owner.

The differences in implementations at the application process levels at the two banks are rather narrow. FSB uses multiple data sources for the matching of addresses whiles the Andhra bank uses a single data source from files. At the Andhra bank, there is currently no effective measures in place for testing the inconsistencies with information received from other credit bureaus but at the FSB, this is given attention and executed effectively.

5.2.2 Analysis: Activation Process

The activation processes at the two banks share some similarities. In both instances when a new card is activated by the customer, they build in fraud controls.

The only difference here is that whereas the process of activation at the Andhra bank is manually carried out, the process is automated at the Foreningssparbanken for the verification of callers' identity.

5.2.3 Transaction behavior monitoring

Monitoring of high-risk situation and transactions is a priority at both banks.

The Andhra bank currently do not have in place any sophisticated system for the monitoring of high risk situation and transactions but at the Foreningssparbanken there is currently in place some sophisticated neural network software which is used to monitor transaction behavior to flag unusual activity. At the Andhra bank, they keep record on individual complains and all such high-risk activity and transactions are typically reviewed against files of the known lost or stolen cards.

5.2.4 Fraud prevention on the Internet

Fraud prevention on the Internet at both banks is a major issue that attracts special management attention. At both banks, a common ground adopted for the combating or preventing fraud on the Internet.

There however some differences in fraud prevention on the Internet at both banks. Foreningssparbanken operates Internet banking in addition to the use of the traditional online credit cards and therefore adopt extra security measures in combating and preventing Internet fraud. The adoption of the Verification Value 2 (CVV2) is one trump card at the Foreningssparbanken. The introduction of the e-card at the FSB is also effective way of addressing Internet fraud, which has contributed to the minimization of credit card frauds at the bank. Whiles Andhra bank continues to experience or witness increase in credit card frauds, the reverse is the situation at the Foreningssparbanken where such incidences has so far been well dealt with.

6. CONCLUSION

This Chapter aims at providing an overall conclusion regarding the findings of this study. This is based on the findings analysis from the previous chapters. We discuss the findings in the first section and the final part looks at suggestions for future research.

The focus of this research has been credit card security in electronic payment. Although a number of security measures were identified and described by both Andhra Bank, India and Foreningssparbanken AB Luleå, Sweden, the consensus from both banks are that security is a threat and would continue to dominate in e-payments discussions in the financial and other credit card issuing companies.

The main research question is:

What security measures can Bank Authorities adopt to secure credit card users details?

- Based on the literature review and coupled with the attempt in finding solution to our research question, as stated in chapter one.

Judging from the above case, security measures in combating credit card frauds in online payments would continue to dominate and attract attention of all stakeholders, thus payment operators, card issuing authorities, merchants and cardholders.

The major advantage of smart cards is the increased security they provide. The chip technology uses sophisticated processing techniques to identify authentic cards and make counterfeiting extremely difficult and expensive. Combining this with a PIN is a proven system for combating fraud as it provides the two-factor authentication of 'something you have' (the smart card) and 'something you know' (the PIN). This makes the probability of fraudulent transactions taking place in an ordinary retail environment extremely low.

Findings from our study indicate that the implementation of effective security measures is capital intensive venture and therefore smaller banks and other financial institutions lacking sound financial backgrounds would continue to struggle in their quest of finding solutions to these problems. The cases of Foreningssparbanken AB, Sweden and Andhra Bank, India provide vivid accounts of the levels of advancement in credit card security.

At the Foreningssparbanken AB, there are virtually no cases of successful credit card break-in frauds after the adoption and implementation of the e-card project initiated by the Swedbank. Credit cards frauds that are so profound at the Andhra bank is effectively dealt with at the FSB. This measure can therefore be said to be effective. At the Andhra bank however, credit card fraud is on the increase. This can be attributed to the continuous exposure of the cardholders' details on credit cards during online payments. These notwithstanding, management at both banks maintain that the frauds in credit cards would continue to pose a major threat with the expansion of e-commerce and other transactions conducted on the internet.

Andhra Bank is having to face up to the realities of the modern highly connected world, which now provides a vast array of opportunities for banks to interact with customers. It has meant that whether as a consumer or a business, the number of transaction channels is now extremely varied and continuing to grow, yet it is not a scenario that all banks are fully prepared for.

At the moment the andhra bank has been established the maximum level of security available to consumers of andhra bank for e-transactions is user ID and password authentication. However, this is already seen as being inadequate for securing financial transactions. Instead, Foreningssparbanken AB banks and credit card providers are turning to the obvious candidate for reducing CNP fraud, the EMV smart card.

The reader here provides the user interface to the card and displays a one-time passcode once it has read the smart card and the user has entered his/her PIN. The user then manually types this passcode into the computer at the appropriate prompt. Only the issuing bank can authenticate this one-time passcode. To avoid repeat attacks, the one-time passcode can also be linked to the individual transaction by a more secure, yet still simple, challenge–response process. In that case, should the passcode be intercepted, it is of no use whatsoever beyond that single transaction.

We are of the firm believe that there is the need for security professionals in all the financial institutions and other credit card issuing companies to always be ahead of the hackers if clients confidence and their own success and reputation.

We also believe that the e-card system from the Swedbank currently in use at the Foreningssparbanken is effective and addresses the problem of credit card details encapsulation by the re-generation of new numbers, CVC2 code and the ability to use the regenerated e-card for just one time transaction.

The e-card system from the swedbank is very effective and with this system we can say that they can reduce the online credit card frauds, so the banks in India like Andhra bank, State Bank of India, Canera Bank, Syndicate Bank, etc and also other banks which are not using this kind of system, these kind of system will be better off if they adopt e-card system to reduce the credit card fraud.

Implications for Future Research:

After the research we found that there is much work done on Electronic Payment System but here we not mostly focus on the Offline payment. We think that this research has enough idea for future researches that include how to be secure from offline payment too. And further research may be one can compare their own banks (their nations bank) to the technically developed bank (like Sweden we say).

REFERENCES

Arata Michael J., 2004: Preventing Identity Theft for Dummies

Basha and Harter, “survey methods”, 1980
http://www.ischool.utexas.edu/~palmquis/courses/survey.html#Resources

Bill Rini., 2002 January-”White Paper On Controlling Online Credit Card Fraud, Window Six. http://www.windowsix.com

Card Fraud Facts 2002, APACS (Administration) Ltd, Association for Payment Clearing Services (APACS), April 2002. http://www.apacs.org.uk

Chris Brenton and Cameron Hunt, 2003: Mastering Network Security; Second Edition

Cristian Radu, 2003: Implementing Electronic Card Payment Systems (Artech House Computer Security Series

creditcards.com, 2006-
http://www.creditcards.com/history-of-credit-cards.php

David S. Evans, Richard Schmalensee, 2003; Paying with Plastic: The Digital Revolution in Buying and Borrowing (Second Edition)

Donal o´mahony, Michael Peirge, Hitesh Tewari, 1997- A text book of “Electronic Payment Systems “

Donal o´mahony, Michael Peirge, Hitesh Tewari, 2001- A text book of “Electronic Payment Systems for E-Commerce”

EzineArticles.com, 2006
http://ezinearticles.com/?Online-Credit-Card-Usage---Convenience-at-its-Best&id=100572

Fink, A., & Kosecoff, J. (1985), “How to Conduct Surveys: A Step-by-step Guide”., Beverly Hills, CA: Sage, 1985

Geoff Lancaster, “Marketing Lectures”.
http://www.da-group.co.uk/main/s6/st72787.htm

How Stuff Works, Inc, 2006
http://money.howstuffworks.com/credit-card2.htm

James Neill, (2004, July 30) - “Qualitative versus Quantitative Research”: Key Points in a Classic Debate.

J.A.N Lee., 1991- “Hacking - Prepared for the Macmillan Encyclopedia of Computers” Professionalism in computer digital library.

John G. Faughnan, “International Net-Based Credit Card/Check Card Fraud with Small Charges”.
http://www.faughnan.com/ccfraud.html#CPBank

John Ross and Sandra Chadwick, 1999- “Research home page”.
http://www.fortunecity.com/greenfield/grizzly/432/Research.htm#

Johnny R. May, 2002: Johnny May's Guide to Preventing Identity Theft:: How Criminals Steal Your Personal Information, How to Prevent it, and What to Do if You Become a Victim

Keith Lamond., 1996 -"Credit Card Transactions – Real World and Online”.

Keith Lamond, 1996
http://www.virtualschool.edu/mon/ElectronicProperty/klamond/CCard.htm

Kurhana A.(1999), Managing complex production processes. Sloan Management Review, Winter, Vol. 40 No. 2

Lavrakas, P. J. (1993), “Telephone Survey Methods: Sampling, Selection, and Supervision”, Newbury Park, CA: Sage, -1993

Linda K. Owens, 2002- “Introduction to Survey Research Design”.
http://srl.uic.edu

Michael D. Myers, 1997 June- “Qualitative Research in Information Systems”.

Nahid Golafshani, (2003 December 4) “Understanding Reliability and Validity in Qualitative Research", the qualitative report, volume-8, pp 597-607

N. Ashokan, Phillipe A. Johnson, Michael Waidner.,1997- “ The State of The Art In Electronic Payment System” A journal of computing practices from IEEE

Online Fraud Report, 2002– “Online Credit Card Fraud Trends and Merchant’s Response”, Mind ware Research Group, Cyber Source. http://www.cybersource.com

Paul Meadowcroft. (2003) Transaction security of the e-Security activities; the Thales Group

Peter Burns, Anne Stanley, “Fraud Management in the Credit Card Industry”.

Proff. Phil Edwards, “What you need to know about credit cards”.
http://www.searcharticles.net/article.cfm/id/939

Ramnath k. Chellappa, Paul A. Pavlou., (2002, 15th November) “Percived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions” A journal of Logistics Information Management, 5/6, v-15, PP 358-368

sandra stammberger,2000- “online credit card usage- convenience at its best”,

S. Peter Buck., 1997- “From Electronic Money to Electronic Cash: Payment on the Net”, A journal of Logistics Information Management, v-10, pp 289-299

Tae-Hwan Shon, Paula M.C. Swatman., 1998-"Identifying Effectiveness Criteria for Internet Payment Systems", A Journal of Internet Research: Networking Applications and Policy, v-8 number 3, pp 202-218

Tej Paul Bhatla., 2003- at. All – "Understanding Credit Card Frauds" Card business review.
http://www.tcs.com/0_whitepapers/htdocs/credit_card_fraud_white_paper_V_1.0.pdf

The Silver Lake 2002: Identity Theft: How to Protect Your Name, Your Credit and Your Vital Information, and What to Do When Someone Hijacks Any of These

Ultimate security solutions for home and office – from fspro labs
http://www.fspro.net/scc/

Vesna Hassler, 2001- "Security Fundamentals for E-commerce", computer security series.

Winston Tellis, 1997; Introduction to case study- The qualitative report, V-3, number 2

Wolfgang Rankland Wolfgang Effing, 2004: Smart Card Handbook (Second Edition)

Yin, R. K, 2002- *Case Study Research, Design and Methods,* 3rd ed. Newbury Park, Sage Publications,

APPENDIX-A

INTERVIEW QUESTIONS

1. Do you work on security?

2. How long have you been working on security in the bank?

3. What aspect of security do you specifically deal with? (Network, Cards, Internet banking or Accounts?)

3. Do you encounter frauds in credit/online cards?

4. How do you detect such frauds?

5. How often do online card frauds occur here?

6. Can you tell us the counter-measures you use to prevent frauds in online cards?

7. In Sweden, customers are always advised not to use their credits directly for? Payment on the internet, but rather use the card to re-generate another card for? payment. Can you tell us how this system functions?

8. How effective has that system be?

9. What advice do you have for your clients who use credit cards as far as security is concern?

APPENDIX-B

Figures and tables-

Current State of the Industry

While the exact amount of losses due to fraudulent activities on cards is unknown, various research analyst reports concur that the figure for year 2002 probably exceeds $2.5 billion. Further, as the overall e-commerce volumes continue to grow and fraudsters adopt more complex schemes, the projected figure for losses to internet merchants in the US alone is expected to be in the range of $5–15 billion by the year 20051. This again is dependent on how rapidly fraud prevention technology will be adopted by the industry. The incidence of fraud for credit card transactions taking place over the internet is according to Garner G22, nearly 15 times higher than face-to-face transactions.

The increased likelihood of fraud, in conjunction with the full economic liability for fraud losses makes risk management one of the most important challenges for Internet merchants worldwide.

Fraud Committed Worldwide

While lost or stolen card is the most common type of fraud, others include identity theft, skimming, counterfeit card, mail intercept fraud and others. Table 1 summaries the modus operandi for credit card frauds and their percentage of occurrence.

Method	*Percentage*
Lost or Stolen Card	48%
Identity theft	15%
Skimming (or cloning)	14%
Counterfeit card	12%
Mail intercept fraud	6%
Other	5%

Table 1: Methods of Credit Card Fraud and their percentage of occurrence

Fraud Category	***2000***	***2001***	***% Change***
Counter feit	107.1	160.3	+50
Card-not-present	72.9	95.7	+31
Lost/stolen card	101.9	114.0	+12
Intercepted in post	17.7	26.7	+51
Fraudulent application	10.5	6.6	+37
Other	6.9	8.0	+15

Table 2: Trend of fraud categories in UK for 2000–2001 (in Pound Sterling millions)
Source:APACS, March 2002

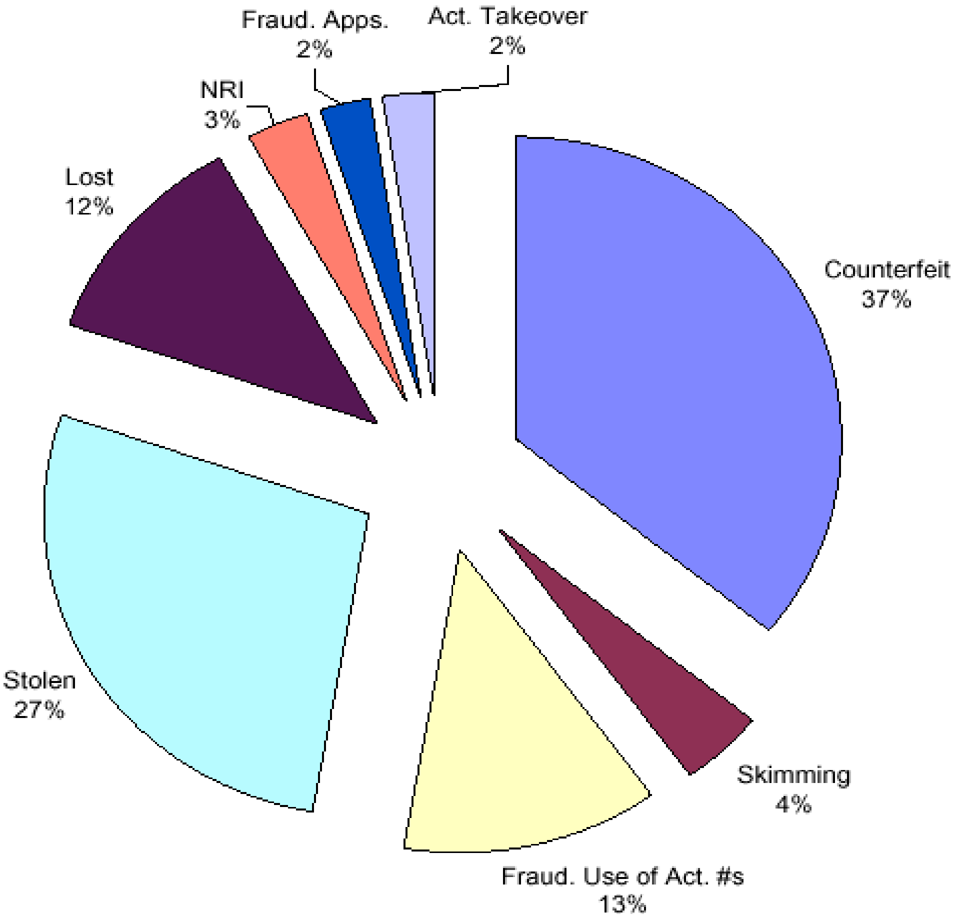


Fig 1.Visa Accounts by Fraud Types for the period of Jan 2001 – May 2001

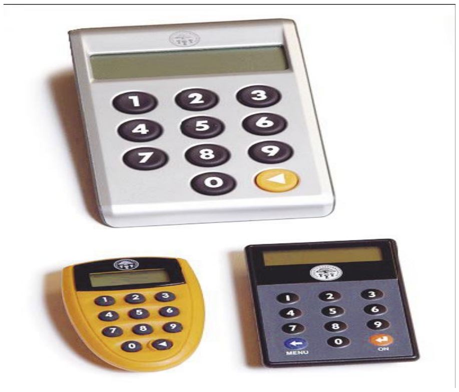
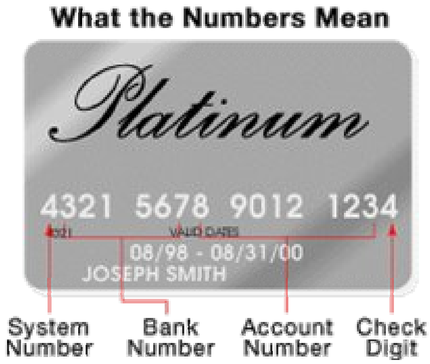
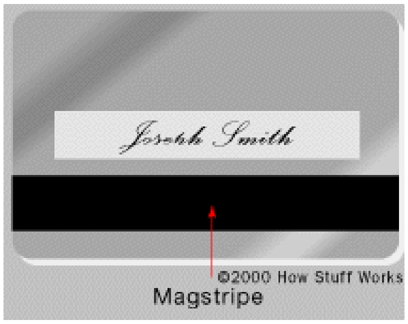


Fig 2. Personal Security Authenticator (PSA) from föreningssparbanken bank

2.11.1 View of the Credit Card

Although phone companies, gas companies and department stores have their own numbering systems, ***ANSI Standard X4.13-1983*** is the system used by most national credit-card systems.





©2000 How Stuff Works

The magstripe can be "written" because the tiny bar magnets can be magnetized in either a north or South Pole direction. The magstripe on the back of the card is very similar to a piece of cassette tape (see How Cassette Tapes Work for details).