JIBC

ARRAY Development

Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, December 2009, vol. 14, no.3 (http://www.arraydev.com/commerce/jibc/)

The Role of IT/IS in Combating Fraud in the Payment Card Industry

Jan Devos
Lecturer at the Ghent University Association, Howest Kortrijk, Belgium
Graaf Karel de Goedelaan 5, 8500 Kortrijk, Belgium
Author's Personal/Organizational Website:
www.pih.be/opleiding/elektronica/~jdv/index.aspx
Email: ***jan.devos@howest.be***

Jan Devos is currently lecturer in Information Systems, IT Management, IT Security and E-Business. He holds a master degree in Engineering and Applied Mathematics and an MBA. He had his own consulting company and conducted more than 50 expert opinions on litigation of IS failures. His current research interest are IT Governance in SME's and IS failures. He has a broad experience as a practitioner in Information Systems Management and Project Management as well as an Executive Professor.

Igor Pipan, MBA
Risk Manager, NLB Tutunska banka AD Skopje, Skopje, Macedonia
Vodnajnska 1, 1000 Skopje, Republic of Macedonia
Author's Personal/Organizational Website: **www. nlbtb.com.mk**
Email: **i.pipan@tb.com.mk**

Igor Pipan is a risk manager at NLB Tutunska banka AD Skopje, involved in fraud prevention related activities in the banks card business. He has been part of the implementation of almost all of the banks card protective systems and is still working in that field.

Abstract

The vast growth of the payment card industry (PCI) in the last 50 years has placed the industry in the centre of attention, not only because of this growth, but also because of the increase of fraudulent transactions. The conducted research in this domain has produced statistical reports on detection of fraud, and ways of protection. On the other hand, the relevant body of research is quite partial and covers only specific topics. For instance, the provided reports related to losses due to fraudulent usage of cards usually do not present the measures taken to combat fraud nor do they explain the way fraud happens. This can turn out to be confusing and makes one believe that card usage can be more negative than positive.

This paper is intended to provide accumulative and organized information of the efforts made to protect businesses from fraud. We try to reveal the effectiveness and efficiency of the current fraud combating techniques and show that organized worldwide efforts are needed to take care of the larger part of the problem. The research questions that will be addressed in the paper are: 1) how can IT/IS help in combating fraud in the PCI?, and 2) is the implemented IT/IS effective and efficient enough to bring progress in combating fraud?

Our research methodology is based on a case study conducted in a Macedonian bank. The research is explorative and will be mostly qualitative in nature; however some quantitative aspects will be included.

The findings indicate that fraud can take up many forms. A classification of the different forms of data theft into different fraudulent appearances was made. We showed that the benefits from implementing the fraud reduction efforts are multiple. Results show that a bank has to be very small to experience losses from fixed expenditures coming from the implementation of the fraud reduction IT/IS. Medium-sized and large banks should not even see any problems arising from those expenditures. Based on the empirical data and the presented facts we can conclude that the fraud reduction IT/IS do have a positive effect on all sides of the payment process and fulfills the expectations of all stakeholders.

Keywords: **IT/IS, Payment Card Industry, Fraud, Case Study**

INTRODUCTION

Since the introduction of the plastic pay card in 1946 by John Biggins, a banker in Brooklyn, the use of cards have steadily grown to large numbers. According to the U.S. Census Bureau there were 159 million credit cardholders in the U.S. in 2000, 173 million in 2006 and that number is projected to grow to 181 million by 2010. (US Census Bureau, 2009). That success leaded to the formation of bank card associations like Mastercard Amex and Visa. Today bank card associations are large international corporations offering standardized services throughout the world. The vast growth of the payment card industry (PCI) in the last 50 years has placed the industry in the centre of attention, not only because of this growth, but also because of the increase of fraudulent transactions. The European Commission reports estimated credit card fraud in European Union is between €500 en €1000 million (APACS, 2008; FPEG, 2009; European Commission, 2008).

The conducted research in the domain of credit card fraud reduction has produced statistical reports on detection of fraud, and ways of protection. On the other hand, the relevant body of research is quite partial and covers only specific topics. For instance, the provided reports related to losses due to fraudulent usage of cards usually do not present the measures taken to combat fraud nor do they explain the way fraud happens. Many different efforts of combating fraud are mostly individual efforts of banks or other organizations directly connected to end customers. This can turn out to be confusing and makes one believe that card usage can be more negative than positive. The motivation behind this research is to shed some light to the worldwide spread fraud problem in the PCI. The PCI gathers payment organizations, as well as banks, merchants and cardholders. Other organizations involved are plastic card manufacturers, terminal and ATM vendors, certification organizations and software providers. So the number of stakeholders that are benefitting from the popularity of the PCI is large. It is therefore paramount that a deep understanding of the overall pay card fraud mechanisms and the IT/IS that can be helpful in combating the fraud, is established.

This paper is intended to provide accumulative and organized information of the efforts made to protect businesses from fraud. We try to reveal the effectiveness and efficiency of the current fraud combating techniques and show that organized worldwide efforts are needed to take care of the larger part of the problem. The research questions that will be addressed in the paper are: 1) how can IT/IS help in combating fraud in the PCI?, and 2) is the implemented IT/IS effective and efficient enough to bring progress in combating fraud?

The remainder of this paper is structured as follows: in the next paragraph we bring an overview of the existing literature on the fraud problem in the PCI, the associated vulnerabilities and the fraud reduction efforts. Paragraph three reveal our research methodology. based on a case study conducted in a Macedonian bank. In paragraph four we show the effects of the fraud reduction efforts. A discussion of the findings is brought in paragraph five and finally in paragraph six we make some conclusions.

OVERVIEW OF THE FRAUD PROBLEM IN THE PCI

The Payment Card System (PCS)

The payment card system stores and transfers data among different stakeholders. The whole process is quite simple and involves five parties, the retailer or ATM, the acquiring bank that installed the POS terminal at the retailer’s or that installed the ATM, the payment organization like MasterCard, Visa, Amex or other, the issuing bank that issued the card and the cardholder initiating the payment (APACS, 2006). The process is shown in figure 1. The cardholder initiates the payment by visiting the merchant location or the ATM with the intention to pay for goods or services or to withdraw cash from the ATM. The cardholders card is swiped on the terminal to obtain the account data. The amount is then entered in the terminal by the merchant or by the cardholder, when cash is withdrawn from the ATM (arrow 1 in figure 1). Data is transferred through the acquiring bank and the payment organization to the issuing bank for verification (arrow 2). The issuing bank verifies or declines the account data as well as the amount requested for payment since the issuing bank keeps constant record of the account balance (arrow 3 and arrow 4). The response is sent back through the payment organization and the acquiring bank to the POS terminal or ATM in form of a response for approval or denial of the transaction. In case of an approval, the funds are debited from the cardholder's account immediately (arrow 5) and transferred later on by the issuing bank to the acquiring bank that transfers the funds to the merchant's account or the ATM's account to balance the same.

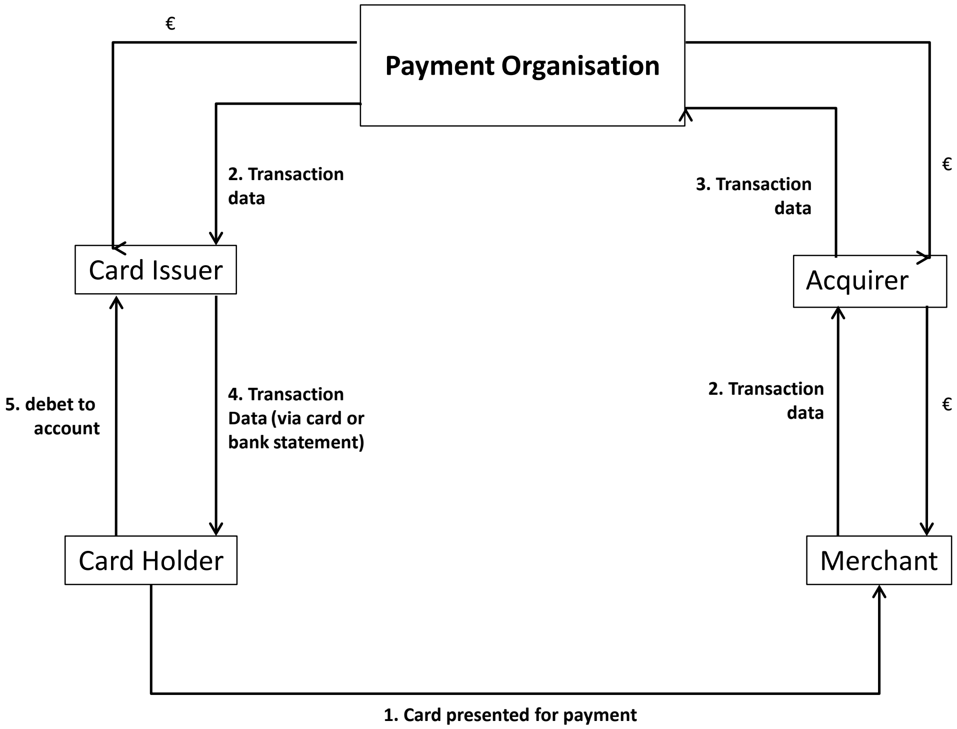

Figure 1 The card transaction process (source: APACS)

All of the parties involved in the PCS keep track of the account data, cardholder data and transaction data for further reference and for the actual fund transfer between the banks. This data is vulnerable and if stolen the data can be used to conduct fraudulent transactions or to produce fake cards.

Vulnerabilities of the Payment Card System

There are many types of fraudulent behaviors, however the terminology can be quite different depending on the organization that classifies the types of fraud. Fraud has also been changed trough time and new types of fraud have occurred. There is no worldwide accepted official classification. Bank card associations use their own classifications which are for internal use only (Visa, 2009; MasterCard, 2009).

The UK Payment Association recognizes five types of fraud: 1) lost/stolen credit card where the card is lost or stolen and then attempted to be used by an unauthorized individual, 2) mail non receipt where the card or cards are being intercepted while being sent to the cardholders by post, 3) counterfeit which is the type of fraud same as skimming, where the card information is copied from the magnetic stripe, 4) card not present where the account information from the card is used to make unauthorized purchases over the telephone or the internet, and 5) card ID theft where the account information is stolen by unauthorized individuals to make fraudulent purchases and can take many different forms. (APACS, 2007).

Another classification comes from Barclaycard, an issuer of at least 12 different types of card products. Barclaycard classifies card fraud in the following categories: 1) counterfeit fraud (skimming), 2) theft or loss of cards, 3) postal interceptions, 4) use of card details, 5) identity fraud, and 6) cash point fraud. The explanation behind the different types of fraud is similar to the previous one, but there are some differences. Counterfeit fraud includes stealing of the credit card data and its usage for production of a clone card. Theft or loss of card includes usage of the original card, stolen or lost one at an acceptance location. Postal interception includes theft of the original card by its interception when posted to the original cardholder’s address. Card detail use includes usage of card data from official card payment documents, like sales slips and card statements, for fraudulent card fund access. Identity fraud includes usage of personal and other information from official banking documents for fraudulent fund access and it does not only include card fraud. Cash point fraud includes card theft and PIN information at cash points for fraudulent usage after the theft and includes techniques for cardholder deception for card and PIN theft. (Barclaycard, 2009).

If we compare this classification with the previous one, we can see that there are no major differences. The main types of fraudulent behaviour are quite the same. The differences occur in the terminology and in the cross-relation of the explanations. Some types of fraudulent behaviour, like counterfeit fraud or skimming and cash point fraud both include theft of card information, but in different ways. Another difference is the introduction of cash point fraud, a type of fraud that does not occur in the official classification from APACS. Cash point fraud, on the other hand, describes just another way to steal card and PIN information, apart from the way described in counterfeit fraud.

Some organizations include also phishing as a type of credit card fraud. Phishing can be seen as theft of vital personal data (Woolsey, 2008).

Since pay card fraud is heavily related to data theft and usage of those data for fraudulent purchases, we can use that fact to try to classify the different fraud types and produce a more organized classification of the different fraud types. We start from the payment system using data to identify and confirm the identity of the cardholder for transaction approval and uses cards to transfer them through the system to identify and confirm the transaction of the cardholder. We can see that there are three sources for data theft, the media used for authentication, the system that transfers data, and the cardholder. Therefore, we could classify the fraud types according to the target of data theft: 1) theft of original card and cardholder information directly from the card, 2) theft of original card and cardholder information directly from the system, and 3) theft of original card and cardholder information directly from the cardholder.

In practice, data theft from the card directly can occur in three ways: data could be stolen by stealing the card, data could be stolen by recording the cards embossing without the cardholder’s knowledge and data could be stolen by reading the data from the card without the cardholder’s knowledge. Therefore, it would seem more practical to split the first fraud type into theft of original card and cardholder information directly from the card by card theft, theft of original card and cardholder information directly from the card by recording the cards embossing and theft of original card and cardholder information directly from the card by card copying

If we take into account what we have previously described, we could classify the different, most common ways to commit crime in the payment card system into: 1) counterfeiting or skimming, 2) theft or loss of cards, 3) card ID theft, 4) identity theft, and 5) cyber crime. In table 1 we present an overview of the fraud types.

Fraud type	*What*	*How*
Counterfeiting	theft of original card and cardholder information directly from the card	ATM, POS or device skimming
Theft or loss of cards	theft or loss of original cards and PINs	Card loss, card theft, card trapping, mail non receipt
Card ID theft	theft of original card and cardholder information directly from the card’s embossing	Card loss, card theft, card trapping, mail non receipt
Identity theft	theft of card, PIN and other information directly from the cardholder	Phishing, social engineering
Cyber crime	theft of card, PIN and information directly from the system	Hacking

Table 1 – Classification of pay card fraud types

Damage from different fraud types

Losses generated by plastic card fraud vary between different countries and regions, depending on many circumstances, among which is card usage. The tendency towards bigger fraud losses would naturally be higher in regions or countries that tend to use plastic cards more. Those countries or regions, on the other hand, could provide a clearer image of the losses that can be generated by plastic card fraud.

UK, a country with a long card usage history and a very well developed plastic card market, has shown that the growth of the fraud losses during one decade, reaching a growth of £382.8 million or 313.7% (APACS, 2007).

Fraud type	*10 year total losses*	*Average loss/year*	*Average rise/year*

Card not present	£ 1.000.300.000	£ 100.030.000	47.2 %
Counterfeit	£ 950.100.000	£ 95.010.000	29.8 %
Lost/Stolen	£ 920.200.000	£ 92.020.000	2.6 %
Mail non receipt	£ 294.100.000	£ 29.410.000	13.0 %
Card ID theft	£ 226.400.000	£ 22.640.000	19.9 %

Table 2 – Plastic Card fraud losses by fraud type on UK-issued cards 1997-2006 (APACS, 2007)

We can easily notice that counterfeit, card not present and lost/stolen represent the highest part of the total losses. Every fraud type, on the other hand, shows a rapid increase during the years, except for the lost/stolen fraud type which shows a minor increase over the years.

The damage presented above is always connected to losses of one of the parties involved in the transaction process. Depending on the transaction circumstances, the cardholder might be reimbursed for the transaction, but then the loss would have to be covered by another party, the merchant or one of the two banks involved in the dispute.

Therefore, determining the motivation behind the protective measures is fairly easy when there are so much parties involved. The PCI is a global business offering services to individuals throughout the world. Those customers rely on the effectiveness of their banks also in the field of security. This pressure from the customers does not end with the banks that issue and service their cards, it continues towards the major card schemes like MasterCard, Visa, Amex and others that connect the banks to the system as their own customers. Since there is more than one customer level, the tendencies and actions for securing the payments are different. Banks are trying to protect their end customers and the card schemes are trying to protect the banks as their customers.

Fraud reduction efforts

There are basically two ways of dealing with the fraud types: prevention and detection. Prevention is possible for some fraud types where an occurrence can easily be predicted. Detection of fraud is done when it is difficult to predict all of the possible ways for the fraud to occur.

Fraud reductions efforts based on prevention are mostly IT/IS solutions combined with organizational measurements. Fraud reduction IT/IS are 3-D secure technology and chip card technology. Organisational measurements are based and inspired from PCI security standards.

3-D secure technology is a protocol used as an extra layer of security for online pay card transactions. It was originally developed by Visa to improve the security of internet payments and offered to customers as the Verified by Visa service (Visa Canada, 2009). Services based on the protocol have also been adopted by MasterCard, under the name MasterCard SecureCode, and by JCB International as J/Secure.

Chip card technology includes usage of smart cards for data carrying, otherwise needed for transaction completion (EMVCo, 2009). The term smart cards refers to cards that use a chip to carry the data and to carry applications that allow the basic functioning of the card along with other services, depending on the offer from the issuer. The term smart card is quite broad though. First of all it can refer to cards that are used outside the PCI, like the ones used for telephone booths. Secondly it can refer to chip cards that allow or do not allow the execution of applications. According to Barge a chip cards can be classified into memory cards and microprocessor cards. Memory cards do not have an embedded processing logic and do not include applications. They only include certain values loaded on to them by the issuer and could include some type of protection logic. Microprocessor cards, on the other hand, have embedded processing logic and could support usage of applications. These are the real smart cards. They operate on the basis of the power supplied by a terminal. The usage also needs a display to operate the applications or functions offered by the card. They include a microprocessor, an operating system and read/write memory that can be updated many times (Barge, 2002).

PCI security standards are an organized effort of the card schemes American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. The creation of the standards and management of the same is left in the hands of a PCI Security Standards Council (PCI Security Standards Council, 2008).

Detection of fraud is organized in a risk monitoring system, mostly supported by IT/IS. A risk monitoring information system (RMIS), in the sense of PCI fraud monitoring is a system that monitors the transactions in the payment network. Since it is usually used individually by every bank, the system monitors the activity of every card issued by the bank and the activity of every terminal, POS or ATM that is installed by the bank. The RMIS follows certain rules to extract transactions that have a certain level of probability of fraud. This action could probably be done manually, but since the system of a medium to large bank authorizes a large amount of transactions in a short period of time, software is needed to assess the fraud probability of every transaction and extract those that have a high fraud probability.

The problem of fraud detection can be seen as a filtering problem and is not an easy task. System automation is even harder to accomplish. This is because the filter cannot give accurate guesses all the time and automation would mean automatic response implementation to the system guesses. Ultimately, this would mean that some of the authentic transactions would be considered as fraudulent (false positives) and the cardholders annoyed with recent checks from the bank that could even block the cards without checking with the customer. Another problem is the efficiency in fraud detection and the identification of rare fraud cases. There is a technical possibility to produce a highly accurate detection system but the costs for such development would be too high and the system would become too complex and generate extra costs later on for new fraud trends adaptation. Most of the systems are therefore developed to handle large amounts of transactions and are oriented towards identification of most fraudulent transactions, but not all. In most cases it is acceptable that the system would bypass some of the fraudulent attempts.

However, researchers and software developers are constantly trying to find new ways to make the system as accurate as possible, keeping in mind the need for simplification. Behind this intention lies the development of Bayesian networks, used for fraud detection that are streaming to replace neural networks, used for fraud detection since the beginning of the 90’s. A neural network is based on finding patterns in transaction variables that indicate fraud (Maes et al., 2002). The risk score calculation is based on simple mathematical functions that evaluate transaction variables and are interconnected using weights that give the final risk score. The training, however, is based on large amounts of data, clearly marked as fraudulent or non-fraudulent transactions, which are used to find patterns and assign weights. A Bayesian network is based on transaction features that are highly indicative of fraud and on calculation of the probability for fraud. The final score is based on the calculation of the probability distribution of all that features individual probability distributions. Because the system is based on probability distribution, it requires smaller amounts of data clearly marked as fraudulent or non-fraudulent transactions for system training. This reduces the time and effort for initial system training and can be used in smaller banks that do not have large amounts of data for training purposes. Furthermore, the system is more flexible and adaptive to new fraud patterns than the neural network system. Finding fraud patterns with neural network systems and assigning weights is an iterative process and requires complete system retrain to find new patterns that have never emerged before and to assign correct weights. Bayesian network systems, on the other hand, do not require complete system retrain. They only require classification of the new transactions as fraudulent or non-fraudulent to extract new features and calculate probability. This is why they are more efficient and require less time and effort to adapt the system after the initial training (Alaric, 2007:1-4).

There are efforts made to make the neural networks more adaptive as well, based on generalization of transaction variables among transactions previously identified as fraudulent. This means extraction of similar transaction variables that would be followed to calculate the risk score for the transaction. The extraction is done on several levels that form buckets of transactions with similar variables. Every bucket carries a certain confidence value which is calculated according to the number of transactions that share the same variable and the total number of transactions. The confidence can be used to calculate the risk score for the transaction. This however, does not make the system adaptive later and still requires complete system retrain to include new fraud patterns (Brause et al., 2009).

Bayesian networks are believed to be more precise in fraud detection than neural networks because neural networks are based on statistics to extract fraudulent transactions, while Bayesian networks are based on probability calculated for every feature identified as fraudulent. Having in mind that they require less training time and are more adaptive to new fraud trends, we can say that they contribute to most of the problems described earlier and are more efficient than neural network based systems (Alaric, 2007).

RESEARCH METHODOLOGY

Our research methodology is based on a case study conducted in a Macedonian bank. The research is explorative and will be mostly qualitative in nature; however some quantitative aspects will be included (Yin, 2004; Myers, 2009). The purpose of the case study is to explore the effects of different fraud reduction efforts implementation that are explained in the previous paragraph.

All fraud reducing efforts require finances for their implementation to return some value for the different parties affected by the fraudulent occurrences. Our most important research question still remains: is the implemented IT/IS effective and efficient enough to bring progress in combating fraud?

To bring some light to the question, we are going to explore the investments made for the implementation of IT/IS for combating fraud. In doing so, we have to make certain assumptions since the pure investments are hard to extract. Almost every investment is connected with features that do not refer to combating fraud only. Sometimes we will also have to make parallels between IT/IS specific for combating fraud and similar ones to bring closer picture to the expenditures.

We explore the benefits from the implementation of IT/IS for combating fraud, both tangible and intangible. Here, we have to make certain assumptions since fraud is very hard to predict. We can never say how much fraud losses will be generated in the future or how many fraudulent attempts will be made. Experience shows that fraud can move from very small to very large amounts within one year solely. We will also try to explore the direct fraud reduction effects from the fraud combating IT/IS.

In the process of exploring the effects of the fraud combating IT/IS, we will use the experience of a Macedonian Bank which is a member of the payment card schemes for more than five years. In the text the bank is referred as ‘the Bank’. The Bank has experienced a vast growth of the payment card business over the years, mostly because of the market circumstances and the need for short-term credits, but also because of the card business organization in which attention has been paid to fraud awareness.

In evaluation of the Banks investments in fraud combating IT/IS we have evaluated four major systems and technologies: PCI Security Standards (PCI SS) 3-D technology, chip technology, and RMIS.

FINDINGS

The PCI SS in the Bank have been implemented several years ago on a processor level and has outsourced its processing operations. The implementation of the PCI SS are a concern of the outsourcer. The security standards are quite broad and concern data security, application security and terminal security.

It is very hard to extract the exact figures for the whole system upgrade since applications and terminals have been used before the implementation of the PCI SS and were purchased from external vendors. Because of this, the applications and terminals upgrade expenditures are hard to provide, even more because vendors make investments and the applications and terminals upgrade has been made for more than one bank and concern the whole market. For the purpose of this case study, we will consider those expenditures insignificant because these expenditures have not shown any major influence on the market prices of the terminals and applications, probably because most of the vendors that have implemented these standards are large organizations who are selling worldwide.

As far as data security is concerned, the experience enlightens us that this can be reached with major differences of components quality. Therefore, there can be major differences in the expenditures. Most of the components were also used on a processor level even before the implementation of the PCI SS. This represents another reason why the security upgrade expenditures are hard to extract. Consequently, we will use information on the appraised expenditures for similar standards implementation, which is the ISO 20000 standard for IT service management and is related to organizational processes that affect security at the same time.

The Bank has been working with two different processing centres until present with major differences in processing quantity. The experience of those processing centres shows that there are major differences in the appraised expenditures for the implementation of the ISO 20000 standard. The first one has evaluated the expenditures on €50.000 and the second one on €750.000. We also have to bear in mind that the number of member banks, connected to those two processing centres is different and that the first one does processing for not more than 5 banks, while the second one does processing for almost 20 banks. As a result, it is quite normal to have differences in the number of processes, especially control processes and to have differences in the overall expenditures. For the purpose of our research, we split the expenditures of the larger processing centre that provides services to 20 banks and use that expenditure on a bank level –€37.500 .

The 3-D technology in the Bank has been implemented partially until this moment on acquiring level so exact figures for that part of the business can be used. Yet, the Bank is currently in the process of negotiation for the implementation of the technology on an issuing level and has also information of these expenditures. The experience of the implementation on acquiring level shows that the major expenditures are connected to a certification process for the technology in the payment card schemes, We refer also to MasterCard Worldwide and Visa Inc., and see that they go up to €30.000 for both payment card schemes. There were also expenditures on a processing level for configuration changes estimated up to €20.000 for both payment card schemes. The implementation proposals on the acquiring level show that the certification costs for the payment card schemes go up to €30.000 which can be extrapolated to the acquiring level. The expenditures on a processing level go up to €15.000 fixed and additional €2.000 per year or €14.000, if we assumed that the technology will be used for 7 years with today's technological changes.

The chip card technology in the Bank has been implemented fully on acquiring level one year ago and partially on issuing level, within one of the two payment card schemes. Nevertheless, we can use precise information of the expenditures since the Bank is currently in the process of certification of the rest of the issuing business. The records show that the process requires certification in the payment card schemes and costs around €30.000 for the issuing part and another €30.000 for the acquiring part for both payment card schemes. The shift towards chip card technology of the issuing part requires change in the personalization method that costs around €50.000. There are some additional costs for chip cards purchase, that would replace magnetic stripe cards, but these are quite low, compared to the rest of the costs and are very hard to predict since they refer to future card purchases after the implementation of the technology, besides the initial purchase. The shift towards chip card technology of the acquiring part requires a change of the terminal software and testing that goes through several iterations till the required functionality of the software is reached and cost around €20.000. Both the issuing and the acquiring part require adaptation of the business processing that costs around €30.000 for each part.

An RMIS is used in the Bank since the beginning of the card business as a leased system from the bank-processing centre. There are monthly costs for its usage, paid to the processing centre. Conversely, here are options for purchase of such software and other system components from certified vendors that costs €100.000, depending on the quality of the used system components and we will employ that cost for the purpose of this research. The overall expenditures, as explained above, are summarized in table 3.

Fraud measure type	***Expenditure type***	***Amount***
PCI SS (ISO 20000)	Approximate total implementation	37.500 €
Subtotal PCI SS (ISO 20000)		**37.500 €**
3-D technology	Total certification	60.000 €
3-D technology	Processing adaptation	49.000 €
Subtotal 3-D technology		**109.000 €**
Chip card technology	Total certification	60.000 €
Chip card technology	Processing adaptation	30.000 €
Chip card technology	Personalization method adaptation	50.000 €
Chip card technology	Terminal software changes	20.000 €
Subtotal Chip (EMV) technology		**160.000 €**
RMIS	Software and system components	100.000 €
Subtotal Risk Monitoring System		**100.000 €**
Total Fraud measure implementation costs		**406.500 €**

Table 3 – Fraud measure implementation expenditures

The overall expenditures, divided into issuing and acquiring expenditures, are given in table 4. We have to consider that the total costs for PCI SS (ISO 20000) are doubled, as the processing adaptation costs for the chip card technology, since they would be applied regardless whether the measures would be implemented on one, or on both sides.

Fraud measure type	***Issuing side costs***	***Acquiring side costs***
PCI SS (ISO 20000)	37.500 €	37.500 €
3-D technology	59.000 €	50.000 €
Chip card technology	110.000 €	80.000 €
Risk Monitoring System	100.000 €	100.000 €
Total costs	**306.500 €**	**267.500 €**

Table 4 – Fraud measure implementation expenditures on issuing and acquiring side

The benefits from the different fraud measures can be looked upon from different angles.

Firstly, we can look upon the total turnover protected by the fraud measures, which can go from €243 million on the issuing side to €271 million on the acquiring side in one year.

Secondly, we have to consider the already recorded fraud as a portion of the turnover. On the issuing side, that fraud amounts up to €65.000 for the period of five years which is 0.005% of the total turnover if we consider only one fifth of the total five year issuing fraud (€13.000). On the acquiring side, that fraud amounts up to €302.000 for the same period, which is 0.022% of the total turnover if we consider only one fifth of the total five year acquiring fraud (€60.400).

In addition, we have to take into consideration that these percentages are very low, compared to industry averages that can go up to 5% fraud of the total turnover. If this was the case in the Bank, than the actual issuing fraud could go up to €12.150.000 per year or €60.750.000 for the period of five years and the acquiring fraud could go up to €13.550.000 per year or €67.750.000 for the same period. The figures of fraud as a percentage of the sales are shown in table 5.

	Issuing side	***Acquiring side***	***Total***
Yearly Sales	€243.000.000	271.000.000 €	302.000.000 €
Actual yearly fraud	€13.000	€60.400	€73.400
Industrial average yearly fraud	€12.150.000	€13.550.000	€15.100.000

Table 5 – Fraud as a percentage of the sales

The “total fraud potential per year” is calculated without the “on-us” transactions that amount up to €212 million for the period of one year. If these were included, then the same transactions would have been calculated twice in the total amount. The “total actual fraud”, though, is calculated without such exclusion since the volume of “on-us” fraud is insignificant. The “total industry average based fraud” is calculated as a percentage (5%) of the “total fraud potential per year”.

The net benefit from the implementation of the fraud combating systems and technologies can be expressed in more than one way, depending on the starting point on which fraud is based.

Initially, if we compare the “total implementation costs” of €406.500 of table 3 with the “total fraud potential” in terms of turnover €302 million (table 5) we will find out that the cost/benefit ratio is 0.13%.

However, the real cost/benefit ratio is the ratio that would include the “actual costs” (€406.500) and the “actual fraud experienced” (€73.400) and results in 5.5381 or 553,81% per year which means that ROI will be experienced in a little more than 5 years time. This result is on the limit of acceptability, since we can assume that the used technology fraud protection technology would probably change within 5-7 years. However, this does not have to be the case since the predecessors of today’s chip card and 3-D technologies, have been used for far more than 5-7 years.

We also have to remember the fact that the actual experienced fraud in the Bank is quite low and below industry averages, as we have mentioned before. If we compare the “actual costs” (€406.500) with the 5% fraud industry average (€15.100.000), we find out that the cost benefit ratio results in 2.69% and that ROI will be reached in the third year of usage of the protective measures, which is more financially acceptable.

As far as the acquiring cost/benefit ratio is concerned, the results are following. The comparison of the acquiring side costs (€267.500) and the acquiring fraud potential per year in terms of turnover (€271.000.000), gives a cost/benefit ratio of 0.0987%. The comparison of the acquiring side costs (€267.500) and the actual acquiring fraud per year (€60.400) gives a cost/benefit ratio of 442.88%, which means that the investment would be returned in 4 years. However, the comparison between the acquiring side costs (€267.500) and the industry based average acquiring fraud (€13.550.000) gives a cost/benefit ratio of 1,97%, which means that the investment would be returned within the first year. These findings are summarized in the table 6.

Cost/Benefit Ratio Type	*C/B Value*	*ROI*
Total costs/total fraud potential (year)	0, 0013	Year 1
Total costs/total actual fraud (year)	5, 5381	Year 5
Total costs/total actual fraud (ind. avg.) (year)	0, 0269	Year 1
Issuing costs/issuing fraud potential (year)	0, 0012	Year 1
Issuing costs/actual issuing fraud (year)	23, 5769	Year 23
Issuing costs/actual issuing fraud (ind. avg.) (year)	0, 0252	Year 1
Acquiring costs/acquiring fraud potential (year)	0, 0009	Year 1
Acquiring costs/actual acquiring fraud (year)	4, 4288	Year 4
Acquiring costs/actual acquiring fraud (ind. avg.) (year)	0, 0197	Year 1

Table 6 – ROI on fraud measures

We also have to take into consideration that most of the expenditures are fixed and that the Bank is a medium sized bank according to the number of cards in circulation, and according to the turnover. Since the number of cards and turnover vary between banks, depending on their size, and most of the costs are fixed (around 60% assumed), there is a bank size under which there is no economic value from the implementation of these fraud protecting measures.

If we assume that the total implementation costs would not go under those 60% and take that amount as the “minimal amount of costs for the implementation” (€243.900), and if we presume that the technologies and systems would have a lifetime of 7 years, we would come to a “total industry average based actual fraud” of €34.842 per year that would make the investment worthwhile. If we deduce that the same “total industry average based actual fraud/actual turnover ratio” would apply, we see that a bank has to have a total turnover per year of €696.857 to make the investment into fraud protecting measures meaningful. Off course, there are always opportunities to implement some of the measures, which is considerable for banks that do not expect a high turnover volume from their card business.

The Bank has implemented all of the mentioned fraud reduction systems and technologies. The effects from some of them can be measured and others can not. For example, the effects from the implementation of the PCI SS cannot be measured directly, as there were no successful hacking attacks made on the bank in the past, for the today’s effects to be measured with. The standards are protecting the core of the business and it would be all or nothing left from the business in case of an attack, depending on whether the standards would serve their purpose and stop the attack or not.

The 3-D technology has also been implemented partially till now, only on the acquiring side. The effects will be seen in a couple of years when the fraud volumes will be measured against the industry averages and when the technology will be implemented also on the issuing side. However, the Bank does not expect any major losses in the future since the technology offers protection of the issuing and acquiring side from direct dispute losses, even if fraud occurs.

Chip card technology has been implemented recently as well, first on the Bank ATMs and now it is in the process of full implementation on the POS terminals on the acquiring side. As far as the issuing side is concerned, the technology was implemented on the Visa brand from the beginning, and currently, it is in the process of implementation on the MasterCard brand.

Results show significant fraud reduction on the acquiring side (ATMs and POS terminals) with no more than 10 fraudulent transactions in the last 6 months on the bank's ATMs. POS terminals show differences between the two brands. While the chip card technology was implemented from the beginning on the Visa brand and is in the process of implementation for the MasterCard brand, it shows major differences in fraud volumes. Actually, there have not been any major fraudulent purchases on the Visa brand on the POS terminals from the beginning, while the MasterCard brand suffers from multiple monthly attacks.

On the issuing side, the Visa brand has had only two fraudulent cases from the beginning, which represents a period of approximately 3 years. The MasterCard brand, on the other hand, has suffered multiple attacks in the same period.

The bank uses a RMIS from the beginning. The effects have not been measured directly, in terms of a number of identified and stopped fraudulent volumes, but fraud attempts have been stopped on the acquiring side, some originating from unknown fraudsters and some from the merchants themselves. On the issuing side, clients have expressed satisfaction from the timely stoppage of card thefts and skimming attempts so far.

CONCLUSION

This research presents the fraud problem and the fraud reduction efforts of the PCI seen from multiple aspects, both qualitative and quantitative ones. We present the PCI functions, as an IS that receives input about payment data, transfers the data to complete the payment, and store them on multiple locations and media. We showed that the system can be subject to data theft. By identifying the most important points for data input, transfer and storage, we extracted the weak points of the system as a basis of fraud appearance – data theft.

We showed that the data theft can take up many forms, depending on the source of the theft and classified the different forms of data theft into different fraudulent appearances. We showed the magnitude of the losses in one of the most developed card economy – U.K., to show how big the fraud problem could be.

The final findings show that the benefits from implementing the fraud reduction efforts are multiple. The organizations that implement them, the banks, are motivated to offer such technologies and information systems to the final customers since the costs for their implementation are bearable costs for the business. The bank has to be very small, from the payment card services point of view, to experience losses from the fixed expenditures coming with the implementation of the fraud reduction information systems and technologies. A medium sized and a large bank should not even see any problems arising from the expenditures associated with the fraud reduction information systems and technologies. The final customers see benefits from the usage of the fraud reduction efforts of the banks, associated with the automation of the fraud protection. The information systems and technologies presented in this work offer an automated response towards fraud protection easing the fraud protection process. The PCI SS offer protection of the whole payment information system, requiring minimal human effort after the implementation. The 3-D and chip technology offer automated fraud protection for the cardholders in the non-face-to-face, as well as face-to-face payment process, not requiring any effort by the cardholder himself. The 3-D technology offers additional protection of the Internet payment process with the usage of passwords that can be different every time the cardholder makes a purchase online. The chip technology makes every communication of the card with the network different. This reduces the requirement for a self-protection instinct of the cardholder, bringing the payment process where it once was, in the zone where cards were seen as an easy way for payment, not as an easy way for losing money. The banks' risk monitoring systems additionally contribute to the fraud reduction and cardholder protection, serving as a backup option, a secondary control of the system. This brings the banks to a new level, as payment card service providers directly associated with the final customers. Besides the role of service providers, they take up role as service protectors, adding to their reputation.

Based on the presented facts we can conclude that, in overall, the fraud reduction information systems and technologies do have a positive effect on all sides included in the payment process, fulfilling the expectations of all of them. Therefore, this work adds to the initiative for implementation of such systems and technologies and most certainly, adds to the efforts for innovation of new ones in the future.

REFERENCES

Alaric, (2007), 'Card fraud detection - Comparison of detection technologies', p. 1-4, [Electronic], PDF.

APACS, (2006), 'The card transaction process', presentation p. 1-2, [electronic].

APACS, (2007), 'Fraud – the facts', PDF p. 4-5, [electronic].

APACS, (2008), '2008 fraud figures announced by APACS', [Online], Available: http://www.apacs.org.uk/09_03_19.htm.

Barclaycard, (2009), 'Credit Card Fraud', [Online], Available: http://www.barclaycard.co.uk/ personal-home/credit-guidance/fraud-guide/what-is-credit-card-fraud/index.html.

Barge, B., (2002), 'Smart Cards', [Online], Spring 2002.

Brause, R., Langsdorf, T., Hepp, M., 'Neural Data Mining for Credit Card Fraud Detection', p. 2, [Electronic], PDF, J.W.Goethe-University, Frankfurt a.M.,Gesellschaft f. Zahlungssysteme GZS, Frankfurt a. M., Germany.

EMVCo, (2009), 'The EMV 4.2 Specification books', Available: http://www.emvco.com/specifications

European Commission, (2008), 'Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU Action Plan', p. 13, [Electronic].

FPEG, (2009), 'Fraud in non-cash means of payment', [Online], Available: http://ec.europa.eu/internal_market/fpeg/non-cash_en.htm.

Maes, S., Tuyls, K., Vanschoenwinkel, B., Manderick, B., (2002), ‘Credit Card Fraud Detection Using Bayesian and Neural Networks’, Proceedings of the First International NAISO Congress on Neuro Fuzzy Technologies, Havana, Cuba.

MasterCard, (2009), ‘Corporate Overview’, [Online], Available: http://www.mastercard.com/us/company/en/docs/012109CorporateOverview.pdf.

Myers, M. D., (2008), ‘Qualitative Research in Information Systems’, [Online], Association for Information Systems, Available: http://www.qual.auckland.ac.nz/.

PCI Security Standards Council, (2008), ‘PCI Quick Reference Guide’, p. (4, 6, 7, 12-24), [Online], Available: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf.

PCI Security Standards Council, (2008), ‘Payment Application Data Security Standard’, v. 1.2., p. 1-22, [Electronic], October 2008.

PCI Security Standards Council, (2009), ‘PCI Encrypting PIN Pad (EPP) Security Requirements’, v. 2.1., p. 1-10, [Electronic], January 2009.

PCI Security Standards Council, (2009), ‘PCI POS PIN Entry Device Security Requirements’, v. 2.1., p. 1-13, [Electronic], January 2009.

U.S. Census Bureau, (2009), ‘Credit Cards—Holders, Number, Spending, and Debt, 2000 and 2006, and Projections, 2010’, [Online], Available:http://www.census.gov/compendia/statab/tables/09s1148.pdf.

Visa, (2009), ‘Visa Inc Corporate Overview’, [Online], Available: http://www.corporate.visa.com/av/pdf/Visa_Inc_Overview.pdf.

Visa Canada, (2009), ‘How VbV works’, [Online], Available:http: //www.visa.ca/en/merchant/ products/vbv/howitworks.cfm.

Woolsey, B., (2008), ‘Credit card 'phishing': What it means, how to prevent it’, [Online], Available: http://www.creditcards.com/credit-card-news/phishing-credit-card-scam-fraud-1282.php [June 20, 2009].

Yin, R. K., (2004), ‘Case Study Research, Design and Methods’, 3rd ed. Newbury Park, Sage Publications.