IDENTIFYING IT SOLUTIONS ON FRAUD IN ELECTRONIC TRANSACTIONS OF FUNDS FROM BANKING SYSTEM

Assist. Marinela Tanascovici Ph.D Student
University of Pitesti
Faculty of Economics
Pitesti, Romania
Ionel Sandu Ph.D Student
University of Craiova
Faculty of Economics and Business Administration
Craiova, Romania
Olimpia Oancea Ph.D Student
University of Pitesti
Faculty of Economics
Pitesti, Romania

Abstract: Although we hear daily of fraud, most of them are not reported. Some reports estimated that approximately 90% of assaults are not reported outside organizations were attacked, and only some of the reports are completed by punishment.In fact, for fear of losing customers, some companies (usually banks and large corporations) prefers to fall to an understanding with attackers in exchange for preserving part of the stolen money and keeping silence. Taking into account the development and modernization of the economies of the world in the last four decades, and simultaneous this global banking development and distribution were strongly influenced by the introduction of new computer technology; in such activities new computer technology had a strong impact on providers and on consumers.

JEL classification: G21, G29

Keywords: IT security, fraud, electronic transactions, banking system

Although we hear daily of fraud, most of them are not reported. Some reports estimated that approximately 90% of assaults are not reported outside organizations were attacked, and only some of the reports are completed by punishment.

In fact, for fear of losing customers, some companies (usually banks and large corporations) prefers to fall to an understanding with attackers in exchange for preserving part of the stolen money and keeping silence.

A progammer assistant from a Swiss commercial bank stole £ 8,000,000 from an account of that bank. Being found, in agreement with the bank management that he won't be brought to justice, he promised not to tell anyone about the intrusion and he retained £ 1,000,000.

Taking into account the development and modernization of the economies of the world in the last four decades, and simultaneous this global banking development

and distribution were strongly influenced by the introduction of new computer technology; in such activities new computer technology had a strong impact on providers and on consumers.

In this context the electronic transfer of funds represents an innovation in payments and is available to consumers through credit cards. These new payment instruments began to replace the existing ones: metal coin, notes, provisions for payment or collection, check with and without limit of amount, treat, promissory notes, etc. This revolution that has occurred in the payment system of economics has the role to streamline cash flow and to enhance the financial circuit responsibility of all economic and commercial banks.

With electronic funds transfer system is currently circulated mostly cash flows from developed countries. Electronic funds transfer system is in fact electronic money circuit.

The card is the payment instrument specific to electronic payment system that allows its holder to pay for goods and services purchased in various trade points and get cash from ATMs, based on existing bank account balance. This payment instrument based on electronics has emerged as an alternative to "traditional payment instruments".

Given the electronic components and wide use of cards, card issuers have certain responsibilities with regarding producing the card and the minimum information that must contain a card.

The cards are vulnerable to loss, theft or counterfeiting. To reduce opportunities for fraud (forgery) were introduced some preventive measures. Card holder must be aware of the need to conduct checks in the use of the card, aiming to prevent misuse and, in turn, the person (company) who accepts payment cards must know the procedures required for use.

One of these measures is the need of a hologram on the card. Holograms were imposed as the most effective set of techniques for providing cards security. Meanwhile, there are certain technical requirements of making cards for wear resistance, safety in design elements to avoid possible removal or modification (e.g. signature). Insurance companies that accept cards, before the transactions must verify whether the signature on the card meets customer's signature on the document signed in procurement, must check the hologram, the validity and integrity of the card.

The TEF[1] system provides an automated means of identification of the person to whom funds are intended (payable). Most systems require for the recognition of the card PIN entry, specific to each customer of the financial institution and which has to be provided to allow the access of a system to a bank account. This code is the only way to protect users, being impossible to know who initiated the transfer because the PIN was used correctly. Therefore it is envisaged too development of other safe means of identification: fingerprints, voice. Smart cards are the most viable alternative methods of providing security.

In TEF's activity are used telephone telecommunication networks, satellite or other means, which are likely to be infected by viruses or intercepted. For example we consider the situation where an ATM device is connected to the computer of the central bank via a telephone line, that could be intercepted and, thus, to achieve routing

[1] Phone company

equipment. Even if communication between the ATM and bank computer is done in code systems, malefactors can decode the information during transmission, as the card number or customer's PIN, which they can use in fraudulent transactions. The same problems can occur in cash transfer through distributors, home-banking terminals and phone.

To prevent such situations, financial institutions have resorted to encoding information provided by telephone. However, the work of coding is very sophisticated and expensive, while coding schemes may be inadequate.

In these conditions were adopted some own security measures, such as limiting the amount and number of cash withdrawals, limiting the number of tests for users who enter incorrect PIN, observing the use of TEF systems to detect suspicious use of cards, insurance (for 24 hours a day) of free phone lines through which customers can notify the issuing financial institution in connection with lost or stolen card.

Frauds can be made even by officials of the bank or its customers. The methods used by them are similar to those of transactions based on documents printed. For example, the official who prepares payroll, create a fictitious person on which, via the TEF, issue a credit on that name to be deposited in his account. Employee fraud can be prevented by simple operational checks at random transactions.

To prevent fraud and for the best possible user information, the National Council of Credit in France suggested that the user to write down your PIN and card number and bank account, so that in case of theft or loss to notify the bank to stop any payments.

Also customers are obliged, in case of theft or lost cards, to notify the bank.

Another important issue to the consumer is concerned with the amount of funds transferred by computer and the existence of documentary evidence of transactions.

ATM devices from the first generation have not provided users written receipts. Right to receive a written document is a prerequisite for the cardholder to have proof of its transaction. Errors and further disputes may occur in any area of banking, but in the electronic system may occur extra problems due to lack of traditional and familiar paper records and due to the fact that the bank may be closed in the moment of the transaction.

So one of the key challenges facing retailers merchants if they wish to implement an electronic trading system, is providing a convenient payment mechanism, perceived as sufficiently safe and easy to integrate into a commercial transaction on-line. Many solutions to this problem have been proposed or used today.

As an alternative to implementing a proper system, the operator can call the Web payment service providers (PSP) or commercial service providers (CSP). The current state of development of electronic commerce, some banks have adopted a proactive stance in terms of e-banking services, others are still reluctant.

Moreover, before granting the status of merchant banks may, in particular smaller companies, to give a sum of money in a collateral account as security for the services to be offered. PSP acts as an intermediary between the merchant and cardholders by providing authorization and payment services online. He enjoys connections with integrated on-line banks and authorizing payments out automatically transfer.

Calling the PSP is a safe solution, and many banks prefer to work with them, making it easier for them to authorize a smaller number of large customers over and take charge of security of payments carried out by companies with which they work.

One of the main impediments that have tempered the growth rate of e-commerce activities is related to security. The essence of the problem is that normally emails are sent unencrypted. In other words, anyone who intercepts them can read the content without problems. For this reason, users are advised not to send credit card details by e-mail.

So identification numbers and card transactions are protected using SSL technology (Secure Socket Layer). This eliminates the possibility for an intruder to obtain the card number, assuming that it intercepts the data as encrypted.

This technology presents also a deficiency i.e.: SSL does not allow the trader to ensure that the person using the card in a transaction is actually its holder. Similarly, SSL does not provide any way to know whether the client of the dealer's website is really authorized to accept credit card payment and is not just a pirate site (fake) designed solely in order to collect data on such cards.

To resolve this problem, MasterCard and Visa promote SET a safer technology developed by uniting the efforts of several interested companies. SET assignment resolves authentication of digital certificates clients and dealer. Furthermore, SET provides greater security than the existing one today on traditional commercial market.

While new means of payment more efficient and also more complex appear, other than credit cards, start to feel the increasingly acute need to call on advice and services provided by specialized companies.

An example is the company S&T Romania Intellinx providing solutions that help financial organizations.

On March 19, 2008-Bucharest, S&T Romania and Intellinx Israeli company, partner in providing solutions for the financial sector, organized with the support of the Romanian Banking Institute, the event "Get Proactive about Internal Fraud" on the solutions for monitoring activities and prevention internal fraud in financial organizations. These solutions are crucial both for internal information security and the public image of the organization.

An Ernst & Young study conducted in 13 European countries showed that about 21% of respondents - financial organizations - have acknowledged that in 2006 faced with the suspicion of "fraud, corruption or bribery" in his company. Intellinx, one of the companies designated by Gartner as "Cool Vendors in Security and Privacy, 2006", builds and provides solutions to protect company information from the dangers and threats from within the organization.

As an argument in this regard in recent months the media has shown instances of fraud identified directly or indirectly.

In most cases, fraudulent came from within the organization and use common tools and commands to his work.

Thus, Intellinx company proposes a new approach to detecting and preventing threats from within, by installing a surveillance system for the original multi-platform, providing full visibility of business user applications organization wide. The system enables organizations worldwide to become proactive against threats from within, while empowering authorized users for any action they take.

Intellinx provides solutions allowing the team members work supervision at business applications based on the model of use, allowing multi-platform analysis, audit and fraud detection in real time. Also, all users can be targeted in a "corporate black box", regardless of access held by registering their interaction with back office systems. As can be played and analyzed the complete user sessions, the search is accomplished using an intuitive search module, type Google. Engine model analysis allows tracking of use and detects in real time occurrence of fraud, using also the tools that minimize the occurrence of false alarms. On this engine can be applied new rules, which were constructed on the basis of fraud identified and there were already registered in "corporate black box".

Using Intellinx solutions supports financial organizations comply with the standards Sarbanes-Oxley, Basel II, privacy regulations on HIPAA, GLBA and the EU Directive 95/46 and the requirement of 10 Payment Card Industry (PCI) Data Security Standard.

"In the 14 years of presence in Romania, S&T has consistently promoted the newest technologies in the world and can help maintain a healthy locally business environment. Intellinx solutions meet stringent requirements for financial organizations. Romanian financial services market expansion combined with the diversification of means of fraud, and cases discussed at length in the press are factors which lead us to believe that the approach to provide Intellinx solutions to our partners that work in the financial sector will help them to enhance their proactive sense and to secure their information with sensitive character." said Bogdan Cocora, CEO S&T Romania.

In turn, Mr. Petru Rares, President - General Director of the Romanian Banking Institute, made some relevant considerations regarding the timeliness and usefulness of the subject presented: "The financial crisis and the recent fraud in international banking system and the new Basel II regulations, the leaders of the bank determines to be increasingly concerned about the need for a fraud scheme to counter the risks of internal fraud and negligence in work. In this context the question of finding a solution to ensure an efficient IT system, including in the same time an anticipation of the behavior of the human factor at risk of fraud. The company Intellinx proposes such a solution for players in the financial market and banking consulting firms, insurance companies, through the use of which organizations can build a specific program that provides fraud strategic approach to align company values the performance."

REFERENCES

1. Black, U. "Internet Security Protocols", Prentice Hall PTR, 2003.
2. McCarthy, L. "IT Security: Risking the corporation", Pretince Hall PTR, NJ. 2003.
3. Miller, M. "Absolute PC Security and Privacy", Sybex Inc., San Francisco-London, 2002.
4. Patriciu, V.V. "Securitatea comunicațiilor", PC Report, pp 20-30, martie 1998.
5. Patriciu, V.V. "Securitatea serviciului WWW, PC Report", pp. 20-28, octombrie 1998.
6. Proctor, E.P., Byrnes, F.C. "The secured Enterprise – Protecting Your Information Assets", Prentice Hall PTR, 2002.
7. Velican, M., "Sisteme de bază de date – Teorie şi practică", Editura Petrion

Lungu, I., Ionescu, S., Muntean, M. Gaudeamus, Bucureşti, 2003.
8. * * * www.snt.ro