Offline Internet Banking Fraud Detection

Vasilis Aggelis
WINBANK (PIRAEUSBANK SA)
aggelisv@winbank.gr

Abstract

Nowadays, most important topic about internet banking is security. Banks' basic concern is ensuring their customers' electronic transactions. Nevertheless, fraudsters are becoming more sophisticated and they act really clever to achieve their target. Having this knowledge, banks try to optimize their detection systems in order to detect fraud and investigate suspect online behavior and transactions. Object of this paper is to demonstrate one successful fraud detection model which is established in Greece. Apart from the offline internet banking fraud detection system itself, which is described briefly, our scope is to present its contribution in fast and reliable detection of any "strange" transaction including fraudulent ones.

1. Introduction

Basic security feature of studied internet banking site is the two factor authorization. When a user conducts a risky financial transaction, in some cases, he has to put a one time password in order to end it.

For user's convenience purposes not all transactions are characterized risky.

We called risky financial transactions, the following ones:

- Funds transfer between bank's accounts.
- Funds transfer from bank's account to any other domestic or international bank's account.
- Massive payments.
- Credit card payment. This payment refers only to credit cards issued by another bank.

Additionally every single user has a standard daily amount limit. That limit concerns only risky transactions and is the same for all users. If the total daily amount of user's risky transactions exceeds limit, then a one time password is needed for transaction completion.

In this security framework acts our detection system. Section 2 contains fraudster's attitude, while in section 3 the set up and function of our offline internet banking fraud detection system is described. Actions taken from bank can be found in section 4 and finally section 5 contains the main impacts from this system.

2. Fraudster Attitude

Fact is that two factor authorizations discourage many candidate fraudsters. Nevertheless, they are not panacea. Fraud never stops.

Fraudsters override security framework, with particular steps. Firstly, they install a Trojan horse in victim's computer. In most cases Trojan horse treats as key logger [2].

The next step is to logon internet banking site, pretending the real user. Fraudster finds out customer's behavior. If the user conducts often funds transfer via internet banking is not appropriate victim.

A fraud convenient victim is someone who uses internet banking only for informational purposes or someone who uses electronic services rarely.

In those cases, fraudster transfers daily amounts nearly to the daily limit. For such amounts one time password is not necessary.

Oblivious victim detects fraud after a long time ago. In this time frame fraudster has made some funds transfers. If time frame is longer than a week, fraudster took a remarkable amount into his account.

3. Set up and Function of Fraud Detection System

Bank took in consideration all parameters which lead in internet banking fraud. Analysts established many detection rules. Apart from the initial ones, new rules are added, when analysis finds out suspect patterns and behaviors. Those rules enhanced in an offline fraud detection system.

System is offline because of its database update. New data are imported in database in constant time frames, not in real time. For time being there is no immediate need to upgrade system in online mode.

Analysis, design and implementation of the system took part in-house. Due to the bank's data sensitivity, one of the prerequisites was in-house set up and function of such system. Data mining [3] and predictive analytics tools contributed in all phases of project and they are part of the system.

Pilot operation period proved system's reliability, accuracy and success. Moreover pilot period helped bank scanning system's bugs, faults and defects. After that period, fraud detection system began to operate in production environment.

Suspect transactions are graduated. Accordingly to their risk, they are signed as high, medium and low risk. Probability of fraud is very low, less than 1% [1]. So the great majority of suspect transactions are not fraudulent. Nevertheless, bank obligates to search all suspect transactions.

Apparently the final target is the online implementation of above described system.

4. Bank's Actions

Special staff receives fraud detection reports. Those people undertake the mission to contact with customers. Communication with internet banking users is a crucial step of the whole process. Many of us consider this communication more important from the system itself.

As we stated in previous paragraph almost 99 in 100 suspect transactions are fraudulent. So in 99 out of 100 cases the agent must not smell fishy. Agent has to talk with customer calmly and friendly, indicating bank's concern for him. There is no need to betray the basic reason for the call. Agent asks customer some questions, reassuring transactions' legitimacy [4].

The main risk of contact is that there is a possibility to frighten customer. In that case customer becomes more infrequent user, and maybe stops conducting internet banking transactions.

When a fraud is reassured, then bank takes all the necessary measures against fraudsters and protects and guarantees its customer deposits.

5. Impacts

Offline internet banking fraud detection system offers many benefits to both bank and customers. Fraud detection system gives added value to e-banking. Especially, nowadays, where fraudsters' attacks are increased considerably in our country, such system differentiate bank owner from other bank competitors.

Bank takes lead. Such in-house system implementations, which are set up for customer benefit, are infrequent in local market.

Fraud detection system indicates quality of e-banking services. Quality depends on user friendly interface, on a full of electronic transactions portfolio, but also depends on user protection and guarantee.

A significant number of users have the sense of care and protection from their bank. This sense helps customer loyalty escalation.

Official fraud victims informed from the bank itself as soon as fraud detected. Customers feel that their bank stands by them and that fact strengthens mutual relation.

6. References

[1] R. Brause, T. Langsdorf and M. Hepp, "Neural Data Mining for Credit card Fraud Detection", *IEEE International Conference on Tools with Artificial Intelligence ICTAI-99*, IEEE Press 1999, pp. 103-106.

[2] V. Aggelis, *The e-banking bible*, New Technologies Publications, Athens, Greece, 2005.

[3] *Using data mining to detect fraud*, SPSS technical report, 2000.

[4] C. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-based Fraud detection Research", *Artificial Intelligence Review*, 2005.