Vladimir Urosevic, PhD
Ministry of Internal Affairs of the Republic of Serbia

UDK:343.533:004+336.17
Pregledni naučni rad

INTERNAL FRAUDS IN ONLINE ENVIRONMENT OF FINANCIAL BANKS

Bank fraud is a crime that has been around as long as banks themselves. Anytime there is a large amount of money floating around, there are going to be people trying to figure out ways to get to it. In developed countries, bank fraud is a serious problem that causes billions of dollars in damages every year. That doesn't mean the banks are the only victims though. Millions of people every year fall victim to monetary damages that are caused by bank fraud. Insider bank fraud is perpetrated by someone who works inside, or has access to restricted areas or information inside of the financial institution. Insider bank fraud can be difficult for banks to defend against, since so many people are put in a position of responsibility with the banks money. The author of this article tries to show the occurrence of internal bank frauds and their forms.

Key words: *Internal bank fraud, online environment, cyber crime*

1. INTRODUCTION

In the business world threat is presented by business-related frauds. Fraud losses cost the financial and retail industries more than $200 billion annually, and industry experts indicate these losses will only increase as criminals and fraudsters become more sophisticated in their approach. To defuse this „bomb", we need to understand fraud trends.

Consumers, merchants and banking institutions are impacted by fraud that can result in identity theft, account takeover and financial loss. The leading fraud threats include malware attacks, SQL injections, skimming, phishing and employee (internal) fraud.

Internal fraud, offline and online, is broadly defined as an employee's misuse or misappropriation of an employer's resources or assets for personal gain. Some authors define this criminal activity as:"Fraud always involves one or more persons who, with intent, act secretly to deprive another of something of value, for their own enrichment" (Davia et al. 2000, pg.143). "The use of one's occupation for personal enrichment through the deliberate

misuse or misapplication of the employing organization's resources or assets" (ACFE, 2006, pg.6). Violations can range from asset misappropriation, fraudulent statements and corruption over pilferage and petty theft, false overtime, using company property for personal benefit to payroll and sick time abuses (Wells, 2005, pg.313).

Online banking has added another channel through which an employee can steal. If a financial institution allows employees access to customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud. Internal fraud can be the most costly to financial institutions.

The potential for fraud can be considered as a set of risks to be managed alongside other risks. Preventive controls and the creation of the right type of corporate culture will help to reduce the likelihood of fraud occurring while detective controls and effective contingency planning can reduce the size of any losses.

About 5 percent of an organization's revenue is lost to these fraud incidents. That translates into a potential total loss approaching $3 trillion a year, according to a report by the Association of Certified Fraud Examiners (ACFE) from april 2010.[1]

The two sectors most stricken by incidents of this type of fraud are two of the most regulated -- banking/financial services and the government/public administration. The problem is that the controls put into place to find and combat many forms of fraud, such as internal audits, are not so effective when it comes to detecting internal fraud.

From most studies results indicated that internal frauds were committed by individuals in one of six departments: accounting, operations, sales, executive/upper management, customer service or purchasing.

For internal fraud alone, the number of investigations at banks and other financial services firms conducted by certified fraud examiners more than doubled during 2008 and 2009 from the prior two-year period, to 298, with a median dollar loss of $175,000 to the institutions, according to the Association of Certified Fraud Examiners from USA. This trend is expected to become even more prevalent as bank fraud continues to rise.[2]

[1] Article: „Fraud & Stupidity Look a Lot Alike"
Available at http://www.bankinfosecurity.com/podcasts.php?podcastID=495 on 10.02.2011.
[2] Article: „Inside Jobs"
Available at: https://www.bankers-bank.com/s3web/1001995/docs/inside_job.pdf on 11.02.2011.

2. SIZE AND RISK DERIVING FROM INTERNAL FRAUDS IN ONLINE ENVIRONMENT OF THE BANKS

Internal fraud is a significant problem to the world economy of today. Organizations allocate lots of resources to internal control, a framework implemented in business practice to prevent internal fraud. These costs, together with the costs of internal fraud itself, represent a large economic cost for the business environment and did not go unnoticed (Jans et all, 2009, pg.1).

From computer viruses to employee theft, fraud is blind to the size or prominence of a company. Since the earliest days of employer-employee relationships, there have been those who have had a reason, an opportunity and a rationalization for stealing from the company they work for. Even with modern awareness and tighter security measures, internal fraud remains one of the areas of greatest potential risk to any organization.

Fraud is most often committed by employees who have financial problems and / or feel that they are somehow "owed" by their employer. Contributing factors can include drug, alcohol or gambling addictions. Common warning signs include a decline in work ethic, personality or life style changes, tips or complaints from others, and analytical anomalies in areas where the employee has access. Examples of these anomalies include:

- Unexplained changes in account balances
- Irregularities in source documents
- Missing or altered documents
- Photocopied rather than original documentation
- Incorrect endorsements on canceled checks
- Excessive debit or credit memos
- Cash shortages or overages
- Excessive late charges
- Unreasonable or changing expenses or reimbursements

Some of the more common forms of insider fraud are:

- **Identity Theft**: When a bank employee steals personal information from customers in order to sell the information or to make fraudulent purchases using a stolen identity.
- **Illegal Insider Trading**: This occurs when an insider has authority to make investments on behalf of the bank, and engages in high risk trades without the bank being aware of it. A series of illegal trades gone wrong can cause enough damage to put a bank out of business.

- **Fraudulent Loans**: Fraudulent loans can occur when a loan officer within a bank forges documents, creates false entities, or lies about the ability of the applicant to repay in order to "borrow" a sum of money from the bank that they never intend to repay.
- **Forged Documents**: A forged document claiming that a sum of money has been transferred to another account or something similar can be valuable to a con artist who doesn't want the bank to notice any missing money.
- **Wire Fraud**: It's common place for banks to wire large sums of money on a daily basis. An insider can fraudulently wire money to a personal account at an offshore bank. It may take a bank months or even longer to notice the missing funds.[3]

2.1. Types of stuff fraud in banks

An unrelated but equally important psychological factor that often directly causes organizations to become victims of fraud is the "trust factor." This is a natural and usually overlooked tendency on the part of management to trust that subordinates are honest, loyal and dedicated and that they would never even *think* of committing fraud. Unfortunately, it is not uncommon for employees to exploit this trust to commit fraud against their employers. Many of these employees are "rookie" criminals—never having stolen from anyone until they committed fraud against their employer. This disheartening reality can exist in an organization's department just as easily as it can occur in operations, sales and marketing or even senior management (Goldman P., 2009, p. 6). By the ocassions they show their activity staff fraud can be devided in several descriptive types such as follows.

The Chancer

Many use their computer skills to test the system – or they may simply press the wrong key. If nothing happens and no one checks up, then they have found a new way to steal from the company. They use this oportunity as criminals by the oportunity.

[3] Article: "Bank Fraud - Attacks From Inside and Out..."
Available at http://www.articlesbase.com/non-fiction-articles/bank-fraud-attacks-from-inside-and-out-233600.html#ixzz1Dwpukl9g on 10.02.2011.

The Collaborator

Within a month of joining, the right sort of new staff member may be inducted in several ways of stealing or invited to join a teft group. Criminal groups especially organized once need people that are a part of system because they can give them exact knowledge on organization or infrastructure of potencial target.

The Rolling Stone

The recidivists changes jobs frequently and has left before his frauds are discovered. This crimes are very often esspecialy because banks dont have mutual cooperation and base of data on people and empoyes with reasons of leaving the company. In many countries there are cases of eployment of stuff that were quited by the banks for internal fraud, and then without any personal checking reemployed in onother bank even on higher management positions.

The Insider

A criminal gang may recuit an existing member of staff or place one of their own within the business to find out how the system work, get access codes and passwords.

3. EARLY WARNING SIGNS THAT INTERNAL FRAUD WAS COMMITED BY THE EMPLOYEE

Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity (HM Treasury, 2011, pg. 29). In many cases it was found that employee were giving some of early warning signs booth subjective and objective. Those signs can be used for early warning of banking security sistem that internal fraud was commited.

3.1. Subjective signs

Subjective signs could be signal that employee is committing something that is not allowed in bank, so he/she could not hide personal reaction as a fear, anxiety etc. This includes unusual ways of communication, material manifestation of unlawful gain, clues of crime that are initial information's for investigation on a level of personal reaction on crime committed etc. Some of this subjective sighs are:

- Employee does not take time off
- Possessiveness of work
- Living beyond their means
- Changes in life style
- Books out of balance
- Missing documents
- Delayed deposits

3.2. Objective signs

Objective signs could be signal that employee is committing something that is not allowed in bank on a material level, with some of evidence that can be characterized as such during the investigation. Those are some of material clues that indicate committing of fraud by the stuff, material manifestation of unlawful acts, clues of crime that are initial information's for investigation etc. Some of this sighs are:

- Records not organized
- Customer complaints
- Altered check items
- Duplicate payments
- Numerous payments to the same individuals
- Need for more petty cash
- Checks payable to CASH

4. DETERRING INTERNAL FRAUD IN ONLINE ENVIRONMENT OF THE BANK

In online environment of banks it is very hard to deterr internal fraud. Criminals from outside a bank aren't the only ones using the latest high-tech schemes; bank employees are also becoming more technically advanced in perpetrating fraud. If duying a bussines you have to have a resonable amount of trust in people that are hired to do the job as best as they can. So, where is that border between the trust and checking employee honesty? Key lies in sofisticated net of preventive mesaures that can be implemented in such a manner to be efective, and jet not to jeperdize trust of employee in company and its management.

Some of this mesaures for prevention can be as follows:

- Assign duties to different people
- Have bank statements available for viewing with restrictions online
- Request documentation for transactions

- Question funds transfers between accounts
- Track credit card bills monthly
- Secure business records
- Know your employees
- Compare employees with payroll
- Reconcile and verify the books monthly
- Know your bank representative
- Back up information and files

The number one detection tool is chance related, like tip-offs and detection by accident. This kind of tool is not easily influenced by corporate governance, because it is linked with corporate culture, and not with controls. The second best detection tool seems to be internal control and is a better candidate for mitigating internal fraud, since it lends itself better to govern. Internal control is currently the most prevalent mean companies use the mitigate fraud.

If we look at the definition, it is clear why internal control is important as a protection against fraud. The achievement of the first category is to encounter transaction fraud, the second to encounter statement fraud and the third category achievement is to protect the organization against fraud for the company. Following this broad definition, internal control can both prevent and detect fraud.

Because of this, financial institutions should require a password or PIN for online banking, and the password or PIN should be stored in an encrypted format. (BITS Fraud Reduction Steering Committee, 2003,pg.9). Another option is to truncate account numbers and customer data and limit employee access to the full numbers.

5. CONCLUSION

Internal fraud is a significant problem to the world economy of today. Organizations allocate lots of resources to internal control, a framework implemented in business practice to prevent internal fraud. From computer viruses to employee theft, fraud is blind to the size or prominence of a company. Since the earliest days of employer-employee relationships, there have been those who have had a reason, an opportunity and a rationalization for stealing from the company they work for. Even with modern awareness and tighter security measures, internal fraud remains one of the areas of greatest potential risk to any organization.

Online banking has added another channel through which an employee can steal. If a financial institution allows employees access to customer data, and that data is the same information needed to gain online access to customer accounts, an employee can easily commit fraud.

Preventive controls and the creation of the right type of corporate culture will help to reduce the likelihood of fraud occurring while detective

controls and effective contingency planning can reduce the size of any losses.

The border between the trust in employee and checking employee honesty lies in sofisticated net of preventive mesaures that can be implemented in such a manner to be efective, and jet not to jeperdize trust of employee in company and its management.

6. LITERATURE

1. **Davia, H.R.; Coggins, P.; Wideman, J.; Kastantin, J. (2000):** *„Accountant's Guide to Fraud Detection and Control"* (2nd Edition), John Wiley & Sons: Chichester, UK, pp. 1-384.
2. **ACFE (2006):** *„ACFE Report to the nation on occupational fraud and abuse Technical report"*, Association of Certified Fraud Examiners, USA, pp. 1-64.
3. **Wells, J. (2005):** *„Principles of Fraud Examination"* John Wiley & Sons: Chichester, UK, pp.1-442.
4. **Goldmann P. (2009):** „*Consultant Report - Outside of P-Cards: Internal Fraud in Accounts Payable and Procurement*", National Association of Purchasing Card Professionals, USA, pp. 1-20.
5. **Jans M.**; **Lybaert N.**; **Vanhoof K. (2009):** *„A Framework for Internal Fraud Risk Reduction at IT Integrating Business Processes: The IFR² Framework",* The International Journal of Digital Accounting Research Vol. 9, Spain, pp.1-29.
6. **Hear Majesty Treasury (2011**): „*Tackling Internal Fraud"***,** Hear Majesty Treasury, UK, pp. 1-37.
7. **The Technology Group for the Financial Services Roundtable** (2003): „*Fraud prevention strategies for internet banking",* The BITS fraud reduction steering committee, USA, pp.1-39.

Internet sites

1. http://www.bankinfosecurity.com/podcasts.php?podcastID=495 on 10.02.2011.
2. https://www.bankers-bank.com/s3web/1001995/docs/inside_job.pdf on 11.02.2011.
3. http://www.articlesbase.com/non-fiction-articles/bank-fraud-attacks-from-inside-and-out-233600.html#ixzz1Dwpukl9g on 10.02.2011.

Dr Vladimir Urošević,
Ministarstvo unutrašnjih poslova Srbije

INTERNE PREVARE U ONLINE OKRUŽENjU U BANKAMA

Prevare u bankama su krivična dela koja postoje toliko dugo koliko i same banke. Svaki put kada se na nekom mestu nalazi velika količina novca u opticaju, biće i ljudi koji pokušavaju da osmisle način kako da prisvoje taj novac za sebe. U razvijenim državama prevare u bankama predstavljaju ozbiljan problem koji uzrokuje milijarde američkih dolara štete svake godine. To ipak ne znači da su banke jedine žrtve ovih prevara. Milioni ljudi svake godine postaju žrtve i trpe finansijske gubitke nastale izvršenjem internih prevara u bankama. Interne bankarske prevare vrše se od strane lica zaposlenih u bankama, koja imaju pristup informacijama banke koje su inače drugima zabranjene i nedostupne ili imaju pristup podacima drugih finansijskih institucija. Borba banaka protiv internih prevare je veoma teška, pošto u njima veliki broj zaposlenih ima pozicije i ovlašćenja da raspolaže novcem banke u svom radu. Autor ovog članka ukazuje na pojavu internih prevara u bankama i njihovih pojavnih oblika.

Ključne reči: *interne prevare u bankama, Online okruženje, kiber kriminal*