I J M I
International Journal of Machine Intelligence
ISSN: 0975–2927 & E-ISSN: 0975–9166, Volume 3, Issue 1, 2011, pp-25-30
Available online at http://www.bioinfo.in/contents.php?id=31

ATTACK VECTORS USED IN FRAUDULENCE CONNECTION DURING ONLINE TRANSACTIONS

PRADEEP PUNDIR AND VIRENDRA GOMANSE
Department of Computer Engineering, Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu Rajasthan, 333001,
*Corresponding author. E-mail: pradeep.pundir@gmail.com

Received: May 11 2011; Accepted: June 06, 2011

Abstract- In today's digital world new technologies are designed for customers. Once this technology becomes a comfort there are risk associated. Online fraud is one of the high risks that are targeting customers, organizations and any individual who wants to be associated with ecommerce transactions. Self Propagating Codes are targeting Personal Identifiable Information of customers during authentication or authorization of any transaction. In this paper emphasis has been given on possible online frauds such as Phishing, Carding and BIN attacks. What are the different attack vectors associated to online frauds and what precautions need to be taken is also briefed in the current article.
Key words – Phishing, Fraudulence Connection

1.1 Introduction

BEWARE OF FRAUDS as Internet is slowly becoming a part of human's life as it increases and used in ones daily life, it is prone to various types of frauds. This paper attempts to make you aware of different kind of digital online frauds and how to protect your money; while you may not have fallen prey to any of them. Digital Online fraud can be defined as someone poses as a legitimate company (that may or may not be in order to obtain sensitive personal data and illegally conducts transactions on the existing accounts. Digital Online frauds are known as "phishing" or "spoofing", the most current methods of online fraud are usually through fake emails, Web sites and pop-up windows, or any combination of such methods.

The main objective of Digital online fraud is to steal "Personal Identifiable Information (PII)" Personal Identifiable information is classified as Full name (first and last name if not common) , National identification number, Primary Account Number (PAN), IP address (in some cases), Credit card numbers , Digital identity , Birthday, Birthplace , Home address, etc. The entire process of stealing PII is known as "identity theft". Identity theft occurs when someone illegally obtains your personal identifiable and uses it repeatedly to open new accounts or to initiate transactions in your name.

Identity theft is a risk which can happen to anyone either online or offline. During Identity theft PII information is stolen from those who do not shop, communicate, or transact online as majority of identity theft occurs offline. PII information is collected either by stealing wallets and purses, intercepting or rerouting your mail, and searching through your trash are some of the common tactics that thieves can. Fig 1 gives an insight of possible Credit Card Frauds. Financial Institutions have started customer awareness via emails, posts, banners at ATM and branches so that as more you are aware about identity theft the better prepared you will be.

Fig. 1- Hierarchy of Credit Card Fraud.

1.2 PHISHING

1.2.1 What Is Phishing?

"Phishing" (pronounced "fishing") occurs when fraudsters use different attack vectors such as e-mail, phone calls, or text messages to try to encourage you to click a link and takes you to fraudulent websites, where you're asked to disclose confidential financial and personal information, like passwords, credit card account numbers and Primary Account Numbers. Phishing is an Internet scam where the user is convinced to provide Personal Identifiable Information.

While the most common type of phish is an e-mail threatening which mostly takes you to a fraudulent log-on page designed to capture your details and lists

consequences if you do not immediately log in and take action, fraudsters may also contact you by telephone or send a text message to your cell phone or PDA.

1.2.2 Different Attack Vectors in Phishing

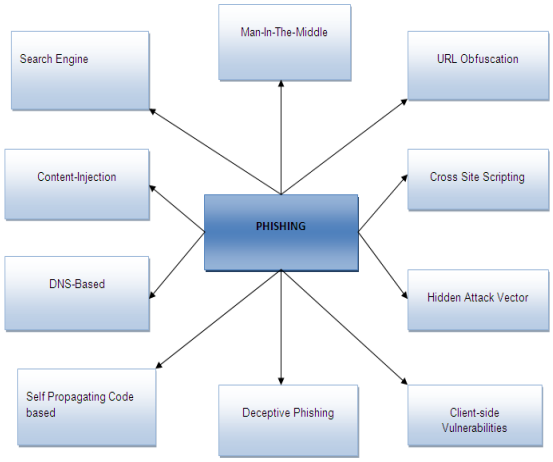


Fig. 2- Attack Vectors in Phishing

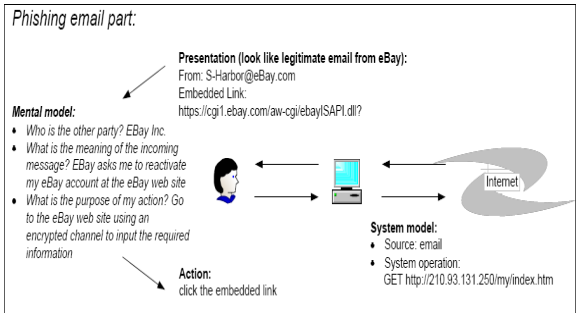
As per Fig.2 different attack vectors in Phishing are highlighted and a summary of each attack vector is summarized below.

- Man-In-The-Middle Attack Vector: In MIMA, the fraudster's computer is placed between the customer's computer and the real website. This helps the fraudster in tracking the communications between the systems.
- URL Obfuscation Attack Vector: The user is made to follow a URL by sending a message which navigates them to the fraudster's server.
- Cross Site Scripting Attack Vector:- This type of attack makes use of custom URL or code to inject a valid web-based application url or imbedded data field.
- Hidden Attack Vector: Attacker uses the HTML, DHTML or other scriptable to change the display of rendered information by interpreting with the customers' web browser.
- Client-side Vulnerabilities:- Most of the customers are vulnerable towards the phishing attacks while they browse the web for any software. These client side vulnerabilities can be exploited in a number of ways similar to the Self Propagating Codes. The IDS or antivirus are not useful for these vulnerabilities as they are harder to identify.
- Deceptive Phishing: The common method of deceptive phishing is email. Fraudster sends a bulk of deceptive emails which command the user to click on the link provided. Fraudster's call to action contains daunting information about the recipient's account. Fraudster than collects the confidential information given by the user.
- Self Propagating Code based Phishing: In this method, fraudster use malicious software to attack on the user machines. This phishing attack spreads due to social engineering or security vulnerabilities. In social engineering, the user is convinced to open an email attachment that attracts the user regarding some important information and download it containing some Self Propagating codes. Exploiting the security vulnerabilities by injecting Self Propagating codes is another form of SPC based phishing.

- DNS-Based Phishing: DNS based phishing is used to pollute the DNS cache with incorrect information which directs the user to the other location. This type of phishing cans be done directly when the user has a mis-configured DNS. The user's DNS server can be changed with a system reconfiguration attack. The users DNS server can be changed with a system reconfiguration attack.
- Content-Injection Phishing: In this attack, a malicious content is injected into a legitimate site. This malicious content can direct the user to soe other site or ir can install Self Propagating codes on the computer.
- Search Engine Phishing: The fraudster creates an identical websites for fake products and gets the pages indexed by the search engine. Fraudster convinces the user to give their confidential information by providing interesting offers.

1.2.3 How the Fraudsters Operate?

Fraudsters uses different techniques such as they send fake e-mails claiming that your bank account or credit card has been compromised, due to which your bank account or credit has been de-activated or suspended, and ask you to hence confirm the authenticity of your Personal Identifiable Information or transactions like credit card number, personal identification number (PIN), passwords or Personal Identification Information such as mother's maiden name, card number, CVV, date of expiry, etc. In order to prompt a response, such e-mails usually resort to using statements that convey an urgent or threatening condition concerning your account.



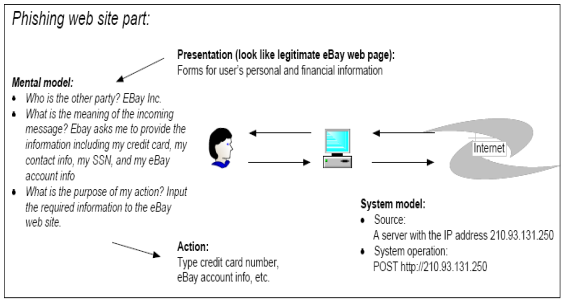


Fig. 3- Real Phishing attacks.

While some e-mails are easy to identify as fraudulent, Fraudsters have fake domain names such that the e-mails may appear to be from a legitimate source. However, you should not rely on the name or address in the "From" field alone, as this can be easily duplicated by various tools.

Fake e-mails may direct you to replicate websites carefully designed to look real. The motive of these websites is to collect Personal identifiable Information from you for misuse; hence these websites are designed and published to look very similar and familiar to you. The rewards that these fake websites or e-mails promise a prize, gift certificate or cash reward in exchange for you're completing a survey or answering a few questions. In order to collect the alleged prize, you may be asked to provide your Personal Identifiable Information. Figure below shows how phishing attacks are carried out by email and website.

1.2.4 Predicting Phishing

- Phishing e-mails mostly may contain spelling mistakes. Even the links to the replicated websites may contain URLs with spelling mistakes, to take you to a fake website which looks like that of your financial institution.
- To offer a job fake e-mails appear to be sent to you by companies. The job profile is more for work at home positions that are actually schemes that victimize both the job applicant and other customers.
- Fake e-mails attempt to convey a sense of urgency or threat. E.g.: "Your account will be closed or temporarily suspended if you don't respond." Or, "You'll be charged a fee if you don't respond.

1.2.5 Tips to Protect Yourself from Phishing

1. Customers should not respond to an e-mail requesting your Internet Banking security details like PIN, password or account number.

2. Take care to check for the URL of the website, whenever you use a link to access a website and try to compare it with the original URL. It is always better to type in the URL yourself whenever you access your bank website or if it's a lengthy URL bookmark/store the URL in your list of 'Favorites'.

3. If the customers feel the e-mails are suspicious delete the suspicious e-mails without opening them. If you happen to open them, do not click any link or attachment of suspicious e-mails unless you know the original source from where it's coming in from.

4. If any job offer is awaited, ensure that it's from a genuine and reputed company.

1.2.6 Comparison Chart: Fraud Attack Vectors

Few statements on phishing attacks by the organizations using encryption as a solution.

(1) While hardware tokens and other physical OTP approaches add a little more protection than simple login/passwords, the physical token value can be easily solicited on phishing websites and reused by the fraudster on the legitimate website. Symantec, the Anti-Phishing Working Group, and numerous other security firms have all noted this vulnerability in published reports.

(2) See Nordea Bank recent inability to stop man-in-the-middle phishing using hardware and similar OTP physical tokens.

	Phishing (Use of fraudulent websites to solicit account credentials)	**Pharming** (DNS poisoning)	**Man-in-the-middle** (Intermediary communication with legitimate website)	**Malware** (Use of malicious software programs to steal computer information)	**Social Engineering and Vishing** (Telephone based and other "in person" fraud)	**Hostile Proxy** (Fraudster's control of a proxy server)
Virtual Token™ authentication	Strong	Strong	Strong	Strong	Strong	Strong
Hardware Tokens, Smartcards, Dongles, etc.	Weak	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Passmark (RSA)-SiteKey	Weak	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Cyota (RSA) - eStamp	Weak	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Business Signatures	Weak	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Digital Envoy (Digital Resolve)	Weak	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable

(3) USB-based hardware tokens, once connected to the customer's computer, are vulnerable to malware which can read and transmit the token values, digital keys, and other data to the fraudster. Non-USB hardware tokens rely on the customer entering Login IDs and other information, including typing the produced token value onto the screen, all of which can be intercepted by malware and transmitted swiftly to fraudsters within the token expiration time frame. Citigroup recently experienced this type of man-in-the-middle attack against its hardware token-equipped business customers.

(4) While "shared secret" approaches add a little more protection than simple login/password approaches, they require users to divulge even more personal information than they would have previously divulged, putting users at even GREATER risk for identity theft. Also, the user's account credentials and personal information can be easily solicited on phishing websites and then re-used by the fraudster on the legitimate website to access the account. Thus, shared secret approaches offer little additional protection and actually increase the probability of identity theft. Symantec, the Anti-Phishing Working Group, and numerous other security firms have all noted these failings in published reports.

(5) Passmark SiteKey's own CTO, Louie Gasparini, confirmed in an recent interview that a "big hole" in the Sitekey approach was its vulnerability to malware,

trojans, viruses or worms. Said Gasparini, "If malware is on your machine, it's much more difficult for everybody." It should be noted that Cyota, Business Signatures, and Digital Envoy, being similar "shared secret" approaches, all suffer from this same vulnerability.

1.3 SPOOFING

1.3.1 What Is Spoofing?

Spoofing is defined as pretending to be someone else and to perform fraud; Website spoofing is done by creating a website by the fraudster. Spoofing is nothing but Phishing where the fraudster wants to obtain personal identifiable information. Spoofing involves names, logos, graphics and even code of the actual website to make it look as legitimate. The fraudsters can even fake the URL that appears in the address field at the top of your browser window and the Padlock icon that appears at the bottom right corner.

1.3.2 How The Fraudsters Operate?

Fraudsters operate by sending e-mails with a link to a spoofed website asking you to update or confirm personal identifiable information. The intention of the fraudster is to obtain sensitive

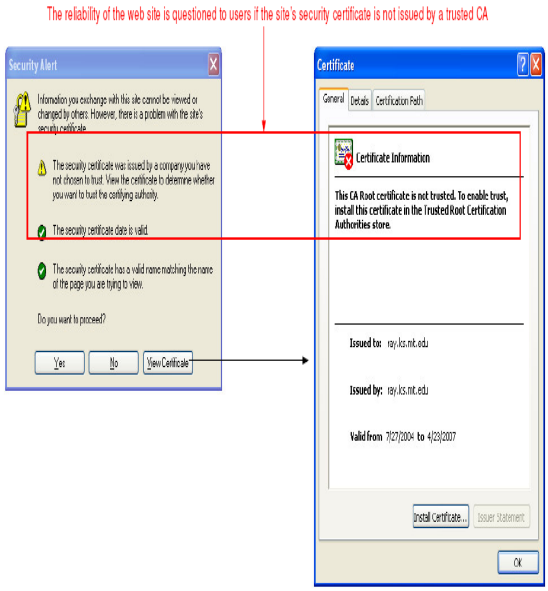


Fig. 5- How to verify SSL/TLS certificate

account related information like Internet Banking user ID, password, PIN, credit card / debit card / bank account number, card verification value (CVV) number, etc.

1.3.3 Tips to Protect Yourself from Spoofed Websites

1. Never respond to an email requesting to reveal Internet Banking security details like PIN, password or account number.
2. Padlock is displayed for any secure connection. If there are any guesses regarding the website; Right Click (or double-click) on it in the web browser to see details of the site's security. It is important to check the certificate validity and authenticity has been issued, because some fraudulent websites may have a padlock icon to imitate the Padlock icon of the browser. Refer to Fig.5
3. URL should be checked when browsing the internet. The URL begins with the letter “http” while browsing and for any secure connection to any financial institute site (example: for confidential transactions) the URL begins with “https” which is nothing but SSL/TSL based transactions.

1.4 VISHING

1.4.1 What Is Vishing?

Combination of Voice and Phishing that uses Voice over Internet Protocol (VoIP) technology is called as Vishing; wherein fraudsters imitate to represent real companies such as financial institution to trick unsuspecting customers into providing their personal and financial details over the phone.

1.4.2 How The Fraudsters Operate?

A typical vishing attack could follow a sequence such as this:

1.4.3 Tips To Protect Yourself from Vishing

1. Do not provide your personal identifiable information to any caller as your bank would have knowledge of some of your personal details. Be suspicious of any caller who appears to be ignorant of basic personal details like first and last name, address, account number, etc. If you receive such a call, report it to your bank.
2. None of the financial institutions ask the customers to call back and provide personal identifiable information on any telephone system that the customers are directed to by a telephone message or from a telephone number provided in a phone message, an e-mail or an SMS especially if it is regarding possible security issues with your credit card or bank account.

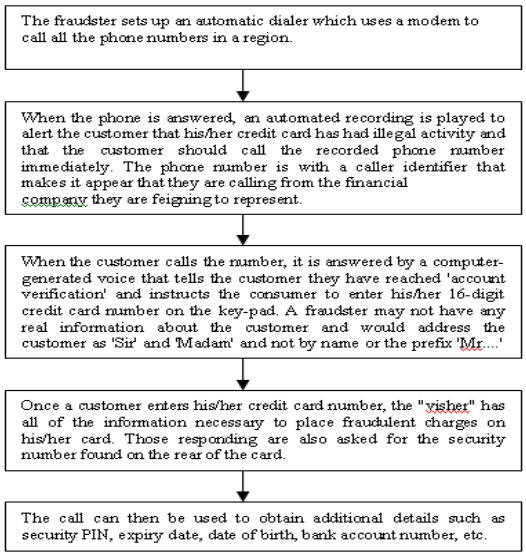


Fig. 6- Real scenario of Vishing attack

3. Always call the helpline numbers provided on back of the financial institution cards to confirm if any fraud or

security issues have been reported by a phone message, an e-mail or an SMS.

1.5 SKIMMING or CLONNING

1.5.1 What Is Skimming?

Skimming is another attack vector of Phishing where the fraudster intention is to capture customer's personal identifiable information of any debit or credit cards. The cards are usually swiped at the skimmer (for customers its just another POS or ATM terminals) and the track information contained on the magnetic strip of the card is read into and stored on the skimmer or any digital storage device. Skimming is used by fraudster to gain track data information from the debit or credit card and recently has gained a lot of popularity.

1.5.2 How The Fraudsters Operate?

- **At ATM machines**

Skimmers are digital devices which are attached to the card slots at ATM machines and are usually used in conjunction with a pinhole camera to read the user's PIN at the same time. While the card user keys in the PIN number for any transaction, the wireless skimming device transfers the data to the fraudster as the device scans the track card information and stores the personal identifiable information.

- **At Restaurants / Shopping Outlets**

The skimmer stores the personal information of any credit card as at restaurants and shopping outlets, the credit card is swiped twice, once for the regular transaction and the other in the skimmer. The personal information is retrieved later by the fraudster.

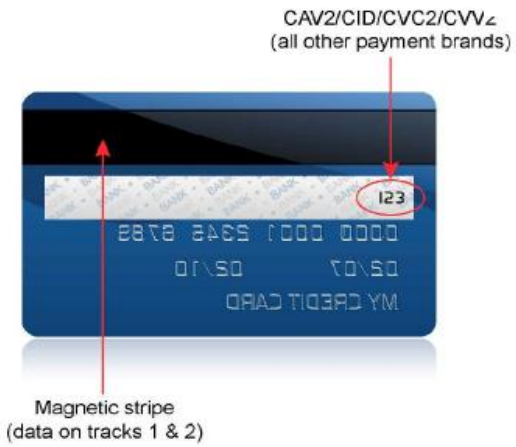


Fig. 7- Details of Credit Card

1.5.3 Tips To Protect Yourself from Skimming

1. Sign on the reverse of your credit card as soon as you receive it.
2. Collect your receipts / charge slips at ATM's, restaurants and shopping outlets.
3. Use your card with merchants that you know and can trust.

1.6 MONEY MULE

1.6.1 What Is Money Mule?

Personal Identifiable Information is captured and stored by the fraudster using anyone of the ways mentioned above, the fraudster now requires an account to which they can transfer funds from the compromised account. This is where a "Money Mule" comes into picture. Money Mule is defined as an unwitting participant in the frauds who is recruited by fraudsters to launder stolen money across the globe.

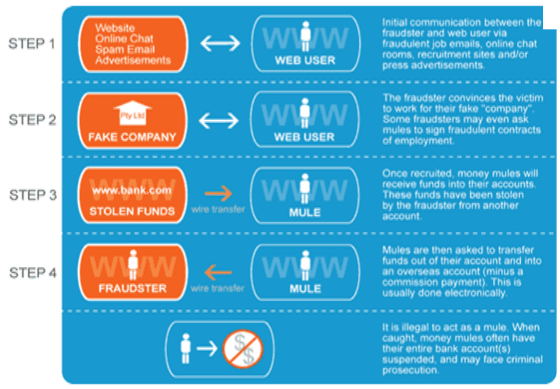


Fig. 8- How Money Mule operates.

1.6.2 How The Fraudsters Operate?

Prospective victims (money mules) are contacted by the fraudster with job vacancy advertisements via spam email, Internet chat rooms or job search Web sites. Jobs usually are advertised as financial management work, and advertisements suggest that no special knowledge is required.

Jobs are offered to prospective victims to come and work for fraudster fake companies. Official looking contracts of employment are signed between the victims and the fake companies. Once the victim is on the payroll or on commission basis of the fake companies money mules receive funds into their accounts. These funds are stolen from financial institution's customers' accounts that have been compromised.

Once the funds are credited from compromise accounts to money mules, then they are asked to take these funds out of their accounts and forward them overseas (minus a commission payment), typically using a wire transfer service or other means. As the account of the mule has been involved in the transaction, the mule also becomes an unwitting participant in the frauds.

1.6.3 Tips To Protect Yourself from Money Mule

1) Offers made by fraudsters to make easy money via e-mails, SMS, banners should be avoided as it's harder to find out the authenticity who they say they are.

2) Fraudster tends to copy a genuine company website and register a similar address to add authenticity to the fraud. The profiles listed on the website or advertisement will state that the company is an MNC or overseas company seeking representatives or agents to act on their behalf for a period of time, sometimes avoid high charges for making payments or local taxes. The goal of

the fraudster is to obtain your account details or Internet Payment Systems.
3) Take steps to verify any company which makes you a job offer and check their contact details (address, phone number, email address and web site) are correct and whether they are registered.

1.7 Carding

Carding is defined as a process used to verify the validity of stolen card data. Carding is performed by the fraudster where he represents the card information on a website that has real time transaction processing. If the card is processed successfully, the fraudster knows that the card is still valid and can be used on the internet for various fraud purposes or illegal means. Item purchased is immaterial as the fraudster does not need to purchase an actual product but a Web site subscription or charitable donation would be sufficient as the purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the card issuer's attention. A website known to be susceptible to carding is known as a cardable website.

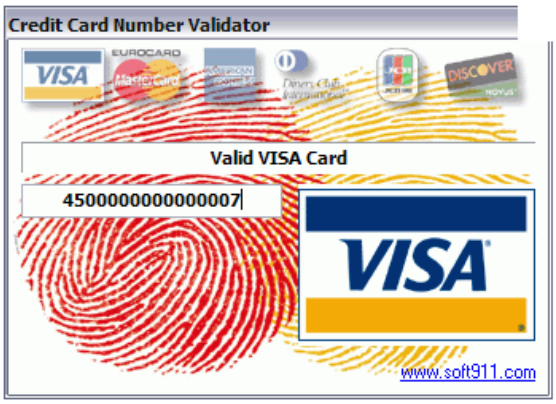


Fig. 9- Card number verification.

Before Carding, "generators" was used as computer programs by carders to produce a sequence of credit card numbers. The fake card numbers were tested to see which were valid by using it on the internet or on any trade shows or places where the cards were not immediately processed. .Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by skimming or phishing.

1.8 BIN attack

In BIN attacks, a valid card number is obtained either via phishing, skimming or other methods and using computer programs called "generators" card numbers are generated in BIN ranges just changing the last four digits. Since the card generated is in sequence the expiry date is likely to be the same as the valid card.

References

[1] Vilalta R., Giraud-Carrier C., Brazdil P. and Soares C. (2004) *International Journal of Computer Science and Applications*,1(1):31–45. DBLP.

[2] Wang S.-N. and Yang J.-G. (2007) International Conference on Machine Learning and Cybernetics, volume 1, pages 283–286.

[3] Washio T. and Motoda H. (2003) *State of the art of graph-based data mining. SIGKDD Explor. Newsl.*, 5(1):59–68.

[4] Wasserman S. and Faust K. (1994) *Social Network Analysis Methods and Applications. Cambride University Press.*

[5] Weiss D. (2006) *Mining customer networks and inter-product relations in internet/ digital entertainment provider data. Master's thesis, University of Zurich.*

[6] Weston D.J., Hand D.J., Adams N.M., Whitrow C., and Juszczak P. (2008*) Adv. Data Analysis and Classification*, 2(1):45–62.

[7] Whitrow C., Hand D. J., Juszczak P., Weston D. J., and Adams N. M. (2009) *Data Min. Knowl.Discov.*, 18(1):30–55.

[8] Wolverton M., Berry P., Harrison I., Lowrance J., Morley D., Rodriguez A., Ruspini E. and Thomere J. (2003) *The Fifteenth Innovative Applications of Artificial Intelligence Conference (IAAI-03, pages* 143–150.

[9] Association of Certified Fraud Examiners (2008) *Report to the nation on occupational fraud and abuse. The Association of Certified Fraud Examiners, Inc., available at http://www.acfe.com/resources/publications.asp?copy=rttn, accessed on January 5th,2010.*

[10] Bankersonline (1992) *Internal fraud. Bankers' Hotline*, Vol. 3, No. 1, 5/92.Available at http://www.bankersonline.com/articles/bhv03n01/bhv03n01a2.html, accessed on January 5th, 2010.

[11] Barse E. L., Kvarnstr ¨om H., and Jonsson E. (2003) *ACSAC IEEE Computer Society*, 384–395.

[12] Becker G. S. (1968) *The Journal of Political Economy*, 76(2):169–217.

[13] Brockett P. L., Derrig R. A., Golden L. L., Levine A., and Alpert M. (2002) *The Journal of Risk and Insurance*,69:341–371.

[14] Burge P. and Shawe-Taylor J. (2001) *J.Parallel Distrib. Comput.*, 61(7):915–925.

[15] Chan P., Fan W., Prodromidis A. and Stolfo S. (1999) *IEEE Intelligent Systems*, 14:67–74.

[16] Chang R., Lee A., Ghoniem M., Kosara R., Ribarsky W., Yang J., Suma E., Ziemkiewicz C., Kern D. and Sudjianto A. (2008) *Information Visualization*, 7(1):63–76.