Risk Management in Electronic Payments

-Electronic Payment Fraud and Digital Forensics

Chia-han Wu
Enterprise Risk Service
Deloitte
Landscape of The Electronic Payment

• Credit card payments
• Automated Clearing House (ACH) and bank payments
• Payment aggregators
• Credit-term providers
• Cash-alternative providers
• Advertising/promotional providers
• Mobile payment providers
• Invoicing payment providers

ADVANTAGES
Privacy
Integrity
Compatibility
Transaction
Efficiency
Acceptability
Convenience
Mobility
Low financial risk
Anonymity
Types of Cyber Fraud that Affect Electronic Payment System

Cyber frauds have grown in complexity and sophistication over years.

The following list covers some of the most commonly faced frauds:
• Trojans that can track user’s activities/hijack SSL Sessions.
• Using a phishing scheme to compromise high net worth clients.
• Using social engineering to compromise a customer and to misappropriate loan funds.
• Using multichannel to compromise a merchant services account.
• Using online channel to compromise a client.
• Using phone channel to compromise a client.
• Fund Transfer Scam emails.
• Insider frauds.
Electronic Payment Fraud 101

• Profile
• The Evolution
• Customer Perspective
• Merchant Perspective
• ID the Perpetrator: Who are they and How do they do it
• Globalization & Cross-Boarder Issues
What Does A Compromise Cost?

- Forensics investigation
- PCI compliance investment
- Card association fines
- Potential authority and other agency fines
- Loss of consumer confidence in electronic payment system
- Actual fraud losses
- Card re-issuance cost
- Bank and association investigation costs
- Cardholder inconvenience
- Adverse publicity – brand and reputation damage
- Legislative interest – threat of governmental regulation
Take a Closer Look at the PCI DSS Requirements, Are They Enough?

- All card accepting merchants must comply with all applicable requirements, below.
- Not all PCI DSS requirements apply to all merchants. Merchants must review each requirement to determine applicability to the merchant’s card payment acceptance systems and business processes.

<table>
<thead>
<tr>
<th>Objective</th>
<th>PCI DSS Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1 Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2 Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3 Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4 Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5 Use and regularly update anti-virus software</td>
</tr>
<tr>
<td></td>
<td>6 Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7 Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8 Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9 Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10 Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11 Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12 Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
Nearly two-thirds of 1,500 executives who chose to respond to a poll said they expected more frauds to be uncovered as the economic downturn continues

- Deloitte Financial Advisory Services’ Anti-Fraud Consulting Services

56% of the companies in the study reported some sort of banking fraud in that last year

- Source Guardian Analytics and Ponemon Institute)
Of those companies, 75% reported that the banking fraud they experienced took place over the internet, and 61% of them claim to have been targeted on more than one occasion.

- Source Guardian Analytics and Ponemon Institute

75% of the businesses participating in the study experienced online account takeover and/or online fraud.

- Source Guardian Analytics and Ponemon Institute
Banks being proactive?

What best describes your bank's response to the online fraud or attempted online fraud?

- 31%: The bank did not compensate my company for any unrecovered funds
- 29%: The bank reimbursed my company fully for any unrecovered funds
- 13%: The bank reimbursed my company partially for any unrecovered funds
- 10%: Money was transferred, but the bank was able to recover all my company's stolen funds
- 9%: Bank discovered the attempted transfer of funds and was able to stop it from occurring
- 8%: Bank was able to identify the account compromise and prevent any transfer of funds
- 8%: 78% of fraud attacks - money left the bank before anyone notices
- 10%: 22% of fraud attacks - stopped proactively by the bank

Source: Guardian Analytics, 2011 Business Banking Trust Study
Both Banks and Businesses are losing money

Source: Guardian Analytics, 2011 Business Banking Trust Study
Customers not giving their institution a second chance

In your opinion, what are the most serious consequences of online fraud or attempted online fraud to your company? Please check all that apply.

- Resulted in the termination of the banking relationship: 10%
- Resulted in our company switching to another bank for primary services: 33%
- Diminished our company’s trust and confidence in the bank’s ability to secure our online accounts: 50%
- Increased our company’s trust and confidence in the bank’s ability to secure our online accounts: 26%
- No affect on the business relationship: 21%

Move their business to another bank - 43%

Source: Guardian Analytics, 2011 Business Banking Trust Study
Cyber Banking Fraud

Major Arrests For using Zeus Trojan horse

The impact of Zeus and other malware

Zeus Malware is the number one threat and primary contributor to the cyber fraud experienced by the entire Financial Services Industry

• Organizations are losing, on average, $100,000 to $200,000 per day due to cyber crime.

• Criminals are primarily stealing money in the financial services industry by using various forms of malware that are designed to exploit security weaknesses in customer computers to initiate fraudulent wire transfer and ACH [Automated Clearing House] transactions.

• Variants (or versions) of the Zeus virus continue to grow each month. In May 2009 alone, 5,079 new variants were launched.

Zeus is extremely difficult to address because there are over 40,000 variants

Source: Kaspersky Lab, Zeus on the Hunt Report, April 12, 2010
Big Challenge for E-Payment

- Anti Identity Theft latest technology: 「Code Card」
  - Simple authentication + virtual keyboard + Two factor authentication + ????
Case I: Fraud Investigation for credit card fraud

According to the requirements of the PCI DSS PFI (PCI Forensic Investigator), DTT assist the Fraud Investigation for global E-commerce.

Chain of Custody

- Check and determine cardholder data that is at risk, includes CAV2, CID, CVC2, CVV2, and/or PIN blocks
- Check volatile memory for cardholder data
- Perform malware analysis and document technical findings on the forensic report
- Other logs that must be reviewed include the following, includes Server, Application, Transaction, Troubleshooting, Firewall, IDS/IPS, Event Logs, Remote Access

Evidence Collection  
Evidence Auditing  
Evidence Handling  
Preservation of Evidence  
Disposal/Destruction of Evidence

Case Study
Case I: Fraud Investigation for credit card fraud

Using Encase, Sleuth Kit and FTK Imager to analyze and investigate the credit card data leakage, examining evidence such as event log of file system, windows registry, system configuration, unallocated disk slack space, and etc.
1) Criminal organization use seemingly SQL Injection attack to E-Payment website that inject the Zeus Trojan malware.

2) Once the webpage is opened, the malware embeds itself into the victims' computers. The malware records the victims' keystrokes which gives the cyber criminal access to account numbers, passwords and other personal data.

3) The cyber criminal uses this information to take over the victims bank accounts.

4) The cyber criminal transfers money to accounts set up with fake identification by money mules - people travelling to the country or on student visas.

5) The money mules keep a percentage of the money - typically 10% - and transfers the rest to cyber criminals.
Case II: Fraud Investigation for Banking Trojans and Money Mules

Hardware and software in real case

Hardware Write Blocker

Antistatic wrist band

Anti static bags

Cyber Crime Investigation Manual

Standard Operating Procedures
For Forensic (Investigating) Expert
Case III: Fraud Investigation for Bust-out fraud

1) A perpetrator applies for a E-Payment Services account and is accepted.

2) Once accepted, the perpetrator exhibits “normal” behavior and processes legitimate transactions for a period of six months.

3) After the initial six months, the perpetrator begins to process fraudulent transactions against the merchant account.

4) In addition, the merchant runs through fraudulent transactions against his/her own bank’s Merchant to enable a “bust-out” scheme.
Case III: Fraud Investigation for Bust-out fraud

1. Data identification
   - Mapping of Electronically Stored Information and paper documents
   - Identification of structured and unstructured data

2. Forensic collection
   - Collect data using forensic preservation standards
   - Maintain chain of custody
   - Perform data integrity check to validate completeness

3. Data fusion
   - Use temporal and entity keys to integrate structured and unstructured data
   - Superimpose data sets to derive context

4. Forensic analytics
   - Apply rules-based detection on 100% of transaction data to identify anomalies (fraud, terrorism threats, etc.)
   - Develop statistically based models to identify previously unknown patterns
   - Optimize anomaly detection rule sets through a feedback loop

New patterns, Risk-ranked, anomalous data sets
Case III: Fraud Investigation for Bust-out fraud
Case III: Fraud Investigation for Bust-out fraud

Deloitte Analytics Tools

Self Organizing Maps (SOM)

Multivariate Model

Neural Network

DTect™ Fraud Detection Tools

Data Governance Framework

Data Model Fit-Gap Assessment Templates
Questions?