



Identifying and Mitigating Cyber Fraud

**Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Atlanta Regional Office**

June 27, 2013





Agenda

Introduction

- **Cyber Fraud Overview**
- **Attack Mechanisms**
- **Mitigation and Best Practice**





Security and Data Integrity Challenges

Methods for stealing personal data and committing fraud are continuously evolving.





Cyber Fraud Threats

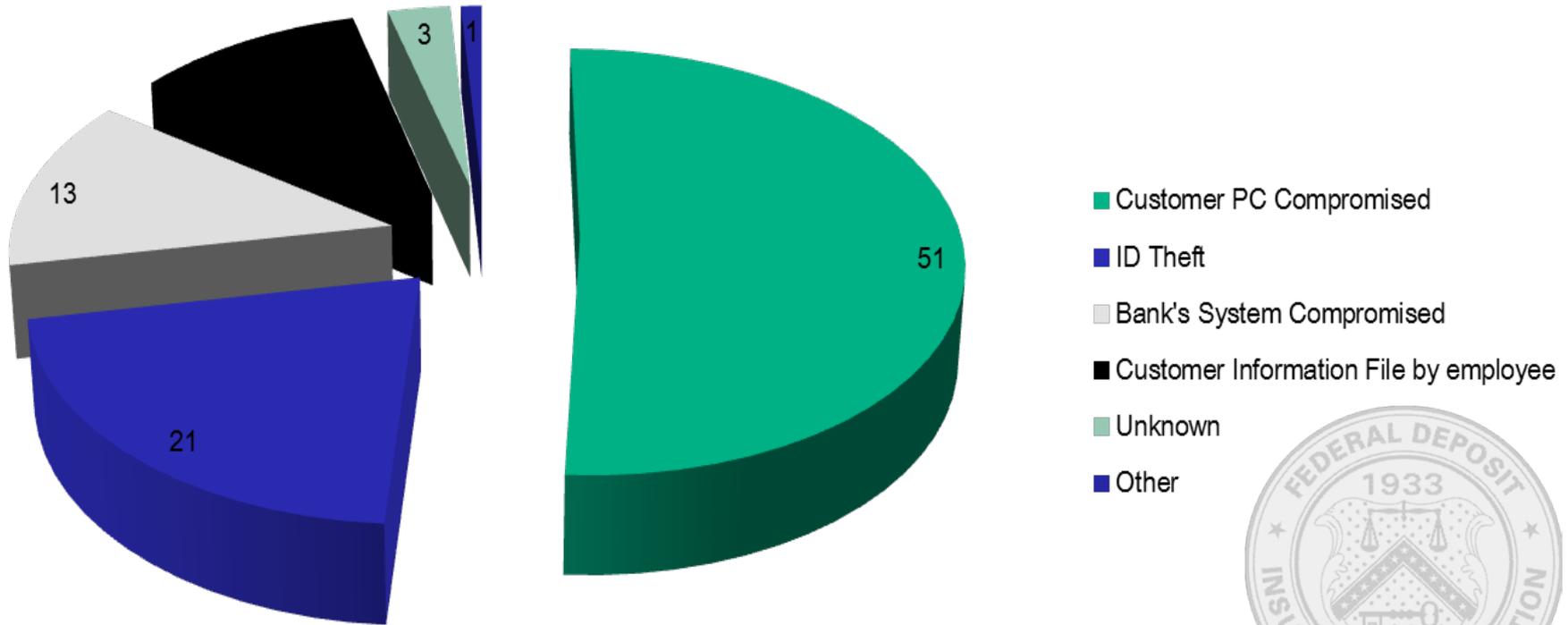
- ACH Credit/Wire Fraud
- ACH Debit Fraud
- ATM Cash-Out
- Database Breach
- Malware
- Denial of Service (DoS)





Computer Intrusion Losses by Origin

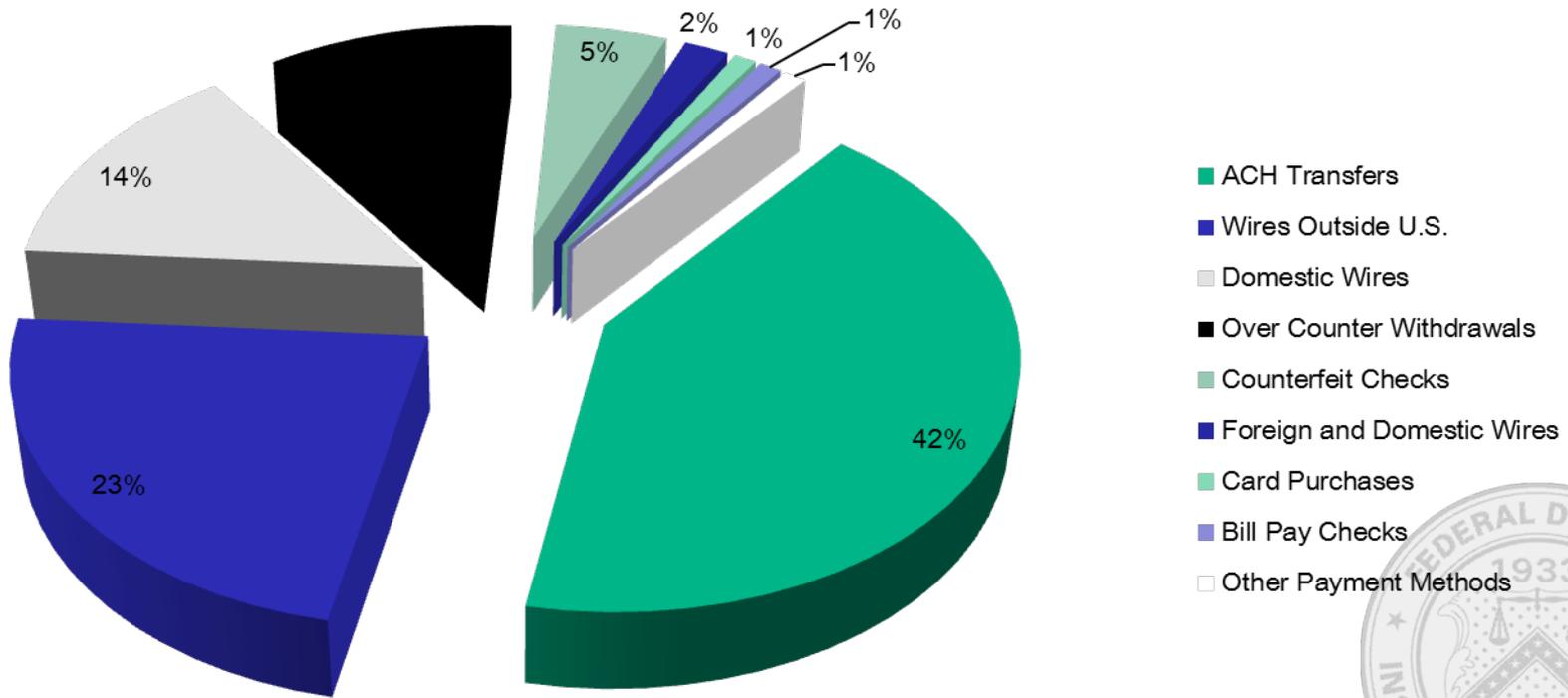
4Q12





Computer Intrusion Losses by Out Flow Method

4Q12





Account Takeover

Account Takeover is a form of identity theft where cyber thieves gain control of a bank account by stealing passwords and other valid credentials. Thieves then initiate fraudulent wire and ACH transactions from the accounts they control.*



* The Texas Bankers Electronic Crimes Task Force



Account Takeover

Methods used to obtain valid online banking credentials include:

Keylogging malware – records legitimate user's keystrokes and sends to perpetrator

E-mail phishing – tricks legitimate user to send credentials or enter them at a web site



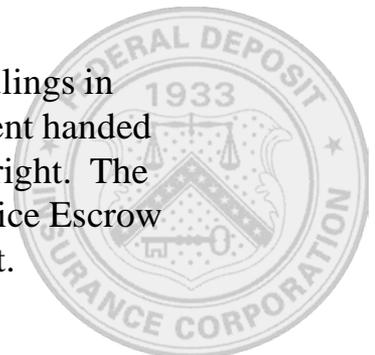


Commercial Account Takeover Lawsuits

Patco: Criminals gained control of Patco's internet banking account and transferred funds via ACH. The bank recovered \$250,000, but held Patco liable for the \$350,000 that could not be recovered. The appeals court found the bank's internet banking security system was unreasonable as a matter of law because the bank permitted the fraudulent ACH transactions even though its risk scoring system identified the ACH transactions as very suspicious.

Experi-Metal: During a six hour period using a phishing attack, cyber criminals initiated fraudulent ACH transactions. The bank was able to recover all but \$560,000 and held Experi-Metal liable for the loss. The company sued the bank and won. The Court held that the bank did not act in good faith since the ACH transactions initiated by the cyber criminals were completely out of character based upon Experi-Metals' typical account activity and was responsible for reimbursing the customer for the \$560,000 loss.

Choice Escrow: Case reflects an evolution in how courts view fraud. Unlike other recent rulings in account takeover cases involving banking institutions and commercial customers, the judgment handed down by this district court favored the bank. This is a case in which the bank did everything right. The magistrate looked at the bank's conduct and found that the bank acted in good faith. The Choice Escrow case went a step further - it asked what obligations the commercial customer should have met.





Mitigating Fraud/Abuse

*Maintain an EFFECTIVE
Information Security
Program (ISP)*





Mitigating Fraud/Abuse (cont.)

Management Accountability

- Central oversight and coordination,
- Assignment of responsibility,
- Risk assessment and measurement,
- Monitoring and testing,
- Reporting, and
- Acceptable residual risk.





Denial of Service

A denial-of-service (DoS) attack or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.





Denial of Service (Continued)

Common symptoms of a DDoS are:

- Degrading web or e-mail resources;
- Increase in network bandwidth usage from your Internet Service Provider;
- Slow network performance; or
- Inability to access some network resources.





Risk Mitigation

- Maintain a current risk assessment.
- Have comprehensive written policies, plans, and procedures.
- Use available security features built into your systems.
- Deploy robust multifactor authentication solutions.
- Limit administrative rights on all devices.
- Deploy available security controls.
- Regularly review security, maintenance, and activity logs/reports.
- Educate employees.
- Implement an effective audit program.





Mitigation (continued)

The DDoS Plan Should:

- Outline the broad requirements for detection, mitigation, remediation and recovery efforts.
- Specify how the response team will be mobilized.
- Ensure timely, accurate and consistent communications.
- Specify the actions to be taken.
- Define post-attack procedures.
- Provide vendor contact information.
- Include processes for contacting regulatory and law enforcement.





Mitigation (continued)

Ingress and Egress Filtering

- Reduces unwanted traffic to your network.
- Analyzes traffic to and from your network.

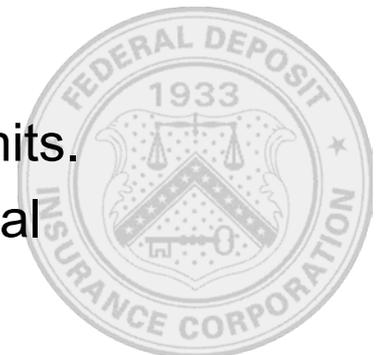




Mitigation (continued)

Know your customers:

- Leverage existing relationship experience,
 - Require customers to complete applications,
 - Understand customer's industry and specific financial trends,
 - Visit customer's site, and,
 - Ensure customer systems are reasonably secure.
-
- Establish comprehensive contracts and agreements.
 - Consider using prefunded or reserve arrangements.
 - Understand customer file submission timeframes and scrutinize outliers.
 - Establish realistic file sizes and transaction exposure limits.
 - Closely monitor customers that are encountering financial and/or operational issues.





Mitigation (continued)

Customer (Public) Awareness and Education

- Recommend customers reconcile/review their accounts on a regular basis.
- Report suspicious activity to the bank and police.
- Consider supporting Public Service Seminars.

Business Continuity and Disaster Recovery Incident Response

- Act immediately when unauthorized transactions are identified.
- Notify your primary regulatory agency when a compromise occurs.
- Consider filing suspicious activity reports.





Mitigation (continued)

Electronic Funds Transfer (EFT)

- Out-of-band and call back procedures.
- Periodic time limits (daily, weekly, etc.).
- NACHA/clearing house rules.

Remote Deposit Capture (RDC)

- Duplicate item detection.
- Use equipment with franking capabilities to minimize errors.
- Review customer due diligence/contracts.
- Report tolerances/parameters/metrics.

Checking

- Monitor check kiting reports.
- Monitor reject/return item reports.





Mitigation (continued)

Post Mortem Supplemental Questions

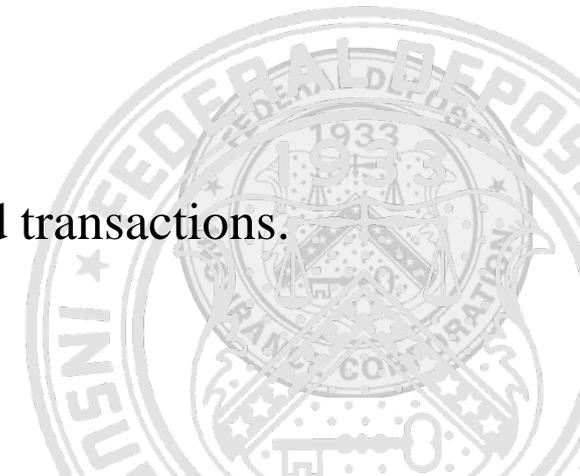
- What parts of your plan were (in)effective?
- How was the quality of your response team?
- Were communications effective inside and outside the organization?
- What controls were (in)effective?
- Were recovery time objectives met? Are there additional measures that can help?
- Was the support from servicers adequate?





Best Practices

- Assess your organization's risk for a DDoS.
- Develop a checklist of actions to take in the event of a DDoS.
- Be familiar with the services your ISP might offer to mitigate a DDoS.
- Consider partnering with service providers:
 - Content Delivery Network (CDN)
 - DDoS Mitigation Service Provider
 - Web Hosting
- Communicate with outside organizations.
 - Financial Services Information Sharing and Analysis Center
- Know your customers and lock out, or hold, unexpected transactions.





Best Practices (Cont.)

- Understand your normal amounts of daily network traffic as well as the performance of your system.
- Separate or compartmentalize critical services:
 - Separate public and private services
 - Separate intranet, extranet, and internet services
 - Create single purpose servers for each service such as HTTP, FTP, and DNS
- Maintain strong change control processes.
- Rate limiting.
- Review US-CERT Cyber Security Tip Understanding Denial of Service Attacks.

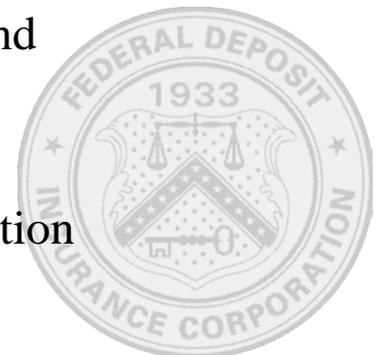




Vendor Management

12 Questions to Ask a DDoS Mitigator

1. How long have you been mitigating DDoS attacks as a service for customer environments?
2. Where do you fit in the DDoS mitigation services market? What level(s) of protection do you offer?
3. How do you protect against attacks that are directed at routers, firewalls, Internet Protocol addresses, and application services directly?
4. Do you monitor our routers for volumetric attacks in the above cases?
5. What protection do you offer protocols other than HTTP, HTTPS, and DNS?
6. What about Virtual Private Network (VPN) endpoints?
7. Do you have Service Level Agreements (SLAs) guaranteeing mitigation within a certain time period?





Vendor Management (cont.)

8. Can you perform real-time analysis of our web traffic and precisely describe what the attack is?
9. How long does it take to push out a filtering rule?
10. Can your staff inspect our Secure Sockets Layer (SSL) traffic manually? What does this mean for privacy?
11. How long does it take for DDoS attack detection and notification?
12. Do you provide detailed attack reports during and after an attack? If after, how long does it take to prepare a report?





Questions





FDIC Contact Information

Thank You!

Richard Snitzer

IT Examination Specialist

FDIC Atlanta Regional Office

rsnitzer@FDIC.GOV

678.916.2224





References

FFIEC Supplement to Authentication in an Internet Banking Environment (FIL-50-2011)

FFIEC Retail Payment Systems Handbook (FIL-6-2010)
Special Alert SA-147-2009: *Fraudulent Electronic Funds Transfers* (August 2009)

FFIEC Guidance on Risk Management of Remote Deposit Capture (FIL-4-2009)

Identity Theft Red Flags, Address Discrepancies, and Change of Address Regulations Examination Procedures (FIL-105-2008)

FFIEC Guidance: Authentication in an Internet Banking Environment (FIL-103-2005)

Payment Processor Relationships-Revised Guidance (FIL-3-2012)

Guidance for Managing Third-Party Risk (FIL-44-2008)

FDIC Supervisory Insights Journal (Quarterly)

National Institute of Standards & Technology (NIST)

Trade Associations (ABA, BITS)

PCI Security Standards Council

US CERT





Sources

- Friedman, I. (2012, July 12) Banking Security: Who is to Blame when Banks Lose Your Money to Fraud? *Examiner.com*. Retrieved April 1, 2013 from <http://www.examiner.com/article/banking-security-who-is-to-blame-when-banks-lose-your-money-to-fraud>
- Kitten, T. (2012, July 9). Inside the PATCO Fraud Ruling. *BankInfoSecurity.com*. Retrieved April 1, 2013 from <http://www.bankinfosecurity.com/inside-pactco-fraud-ruling-a-4927/op-1>
- Kitten, T. (2011, December 30). Account Takeover: Better or Worse? *BankInfoSecurity.com*. Retrieved March 28, 2013, from <http://www.bankinfosecurity.com/account-takeover-better-or-worse-a-4368/op-1>
- Kitten, T. (2011, July 29). ACH Fraud: Comerica Pays Settlement. *BankInfoSecurity.com*. Retrieved March 28, 2013, from http://www.bankinfosecurity.eu/articles.php?art_id=3905
- Vijayan, J. (2010, February 12). Michigan firm sues bank over theft of \$560,000. *Computerworld.com*. Retrieved May 17, 2010, from http://www.computerworld.com/s/article/9156558/Michigan_firm_sues_bank_over_theft_of_560_000
<http://www.prolexic.com/knowledge-center-how-to-choose-a-ddos-protection-provider.html>

