Identifying and Mitigating Cyber Fraud

Federal Deposit Insurance Corporation
Division of Risk Management Supervision
Dallas Regional Office

May 9, 2013

Agenda

Introduction

Cyber Fraud Overview

Attacks

- Account Takeover
- Wire
- Card

Mitigation/Best Practice

Denial of Service

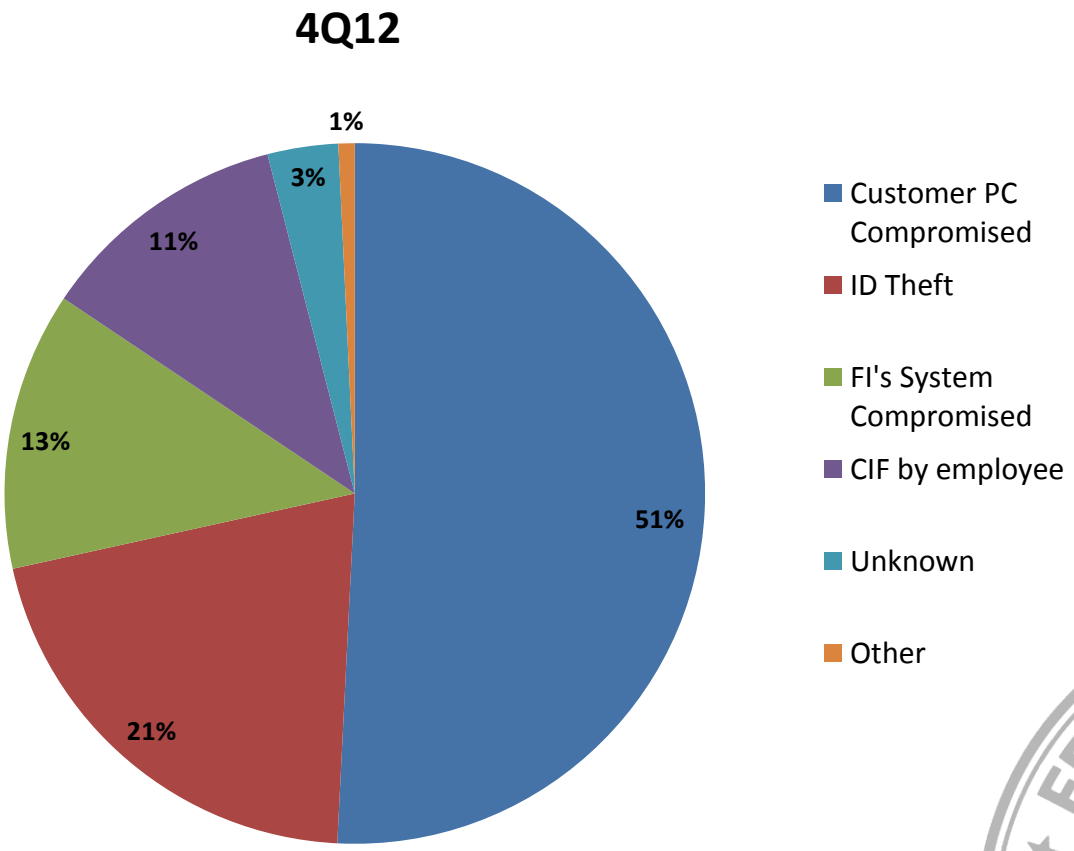
Security and Data Integrity Challenges

Despite generally strong controls and practices by financial institutions, methods for stealing personal data and committing fraud are continuously evolving.

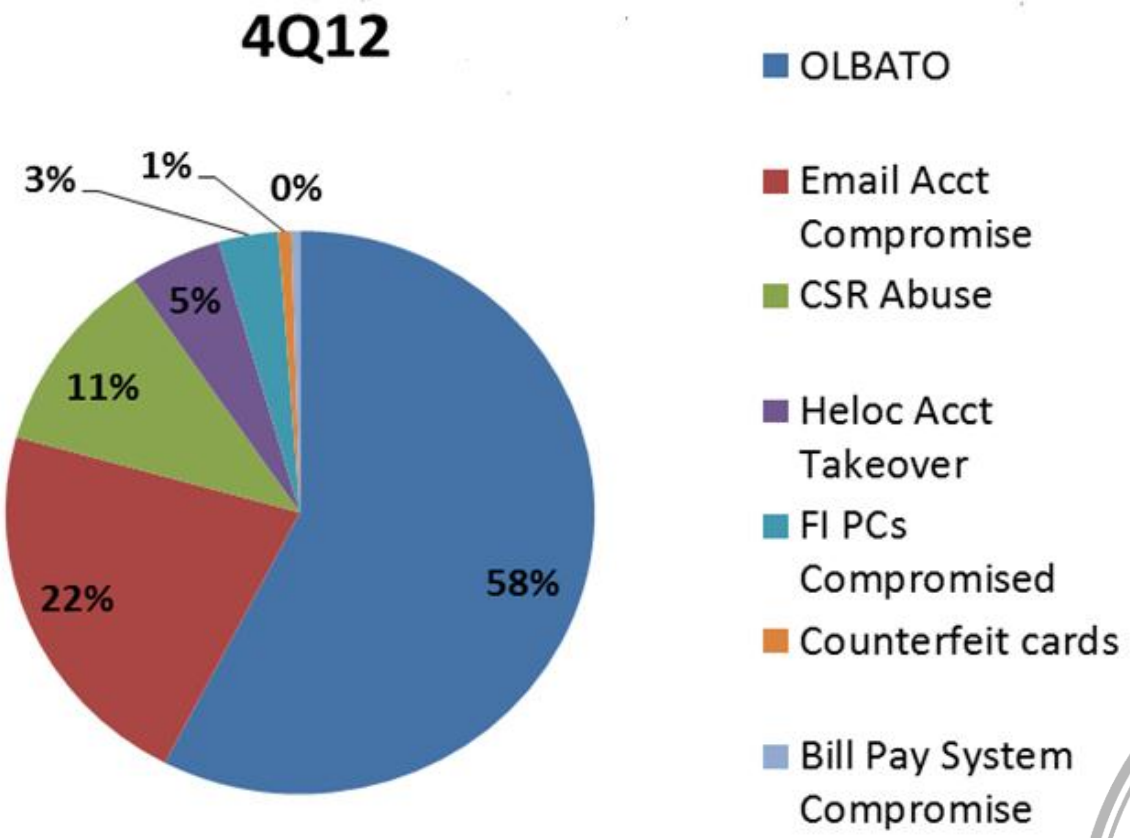
Cyber Fraud Threats

- ACH Credit/Wire Fraud
  (aka “High Roller” attacks)
- ACH Debit Fraud
- ATM Cash-Out
- Database Breach
- Denial of Service (DoS)
  – Social Media Flash Attacks
- Malware

Computer Intrusion Losses by Origin

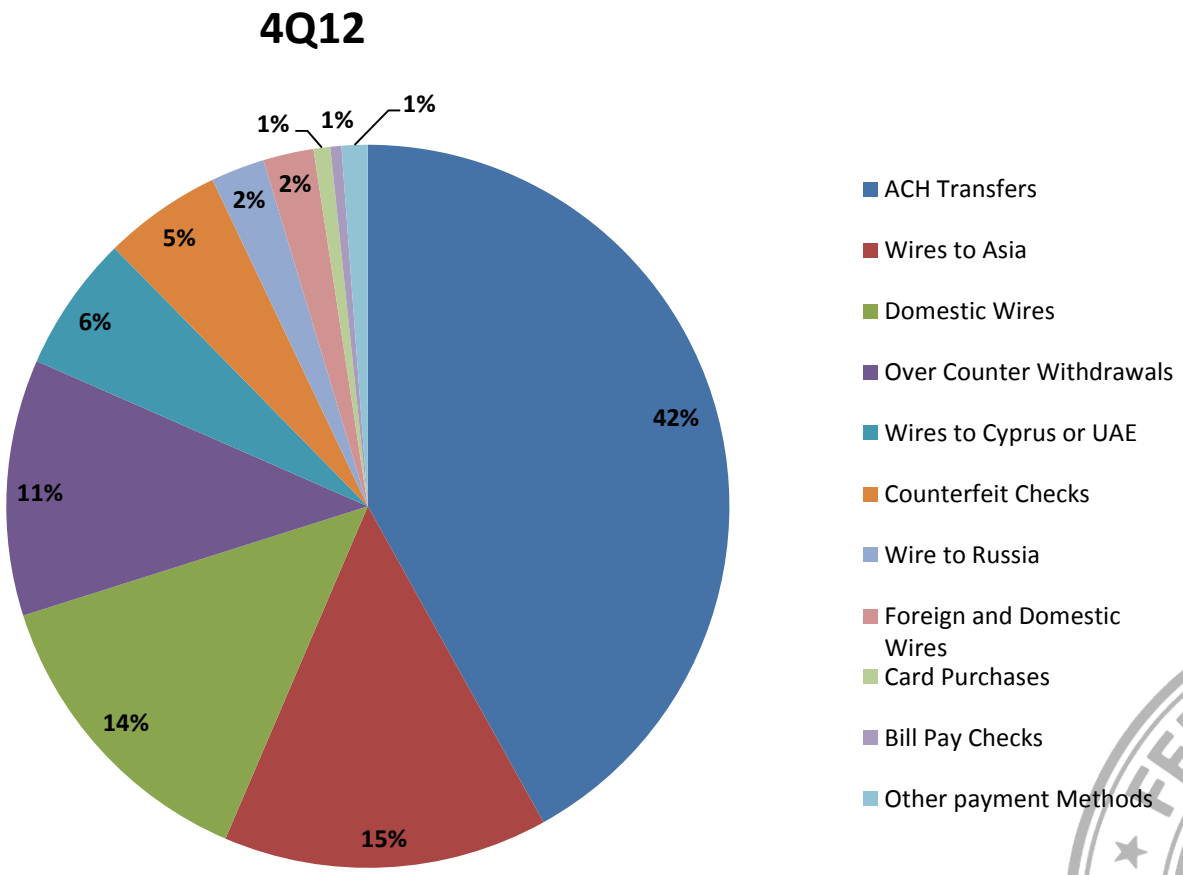


Computer Intrusion Losses by Event Type



* OLBATO – OnLine Bank Account Take Over

Computer Intrusion Losses by Out Flow Method



a shift to *DIFFERENT* targets

2010 and earlier:

Credit card numbers

2011 until now:

Hackers now prefer

<u>USER CREDENTIALS</u>

* InfoSec World 2013: “Trends in Cyber Threats: Who, What, How, Why”

A few statistics about users

- 60% will insert a found thumb drive into their desktop/laptop
- 90% if it has a company logo on it
- More than 50% will give up their passwords in exchange for a token gift
- 90% share passwords across accounts
- 41% share passwords with others
- 14% have never changed their banking password

* Source: Webroot, Trend, McAfee

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.*

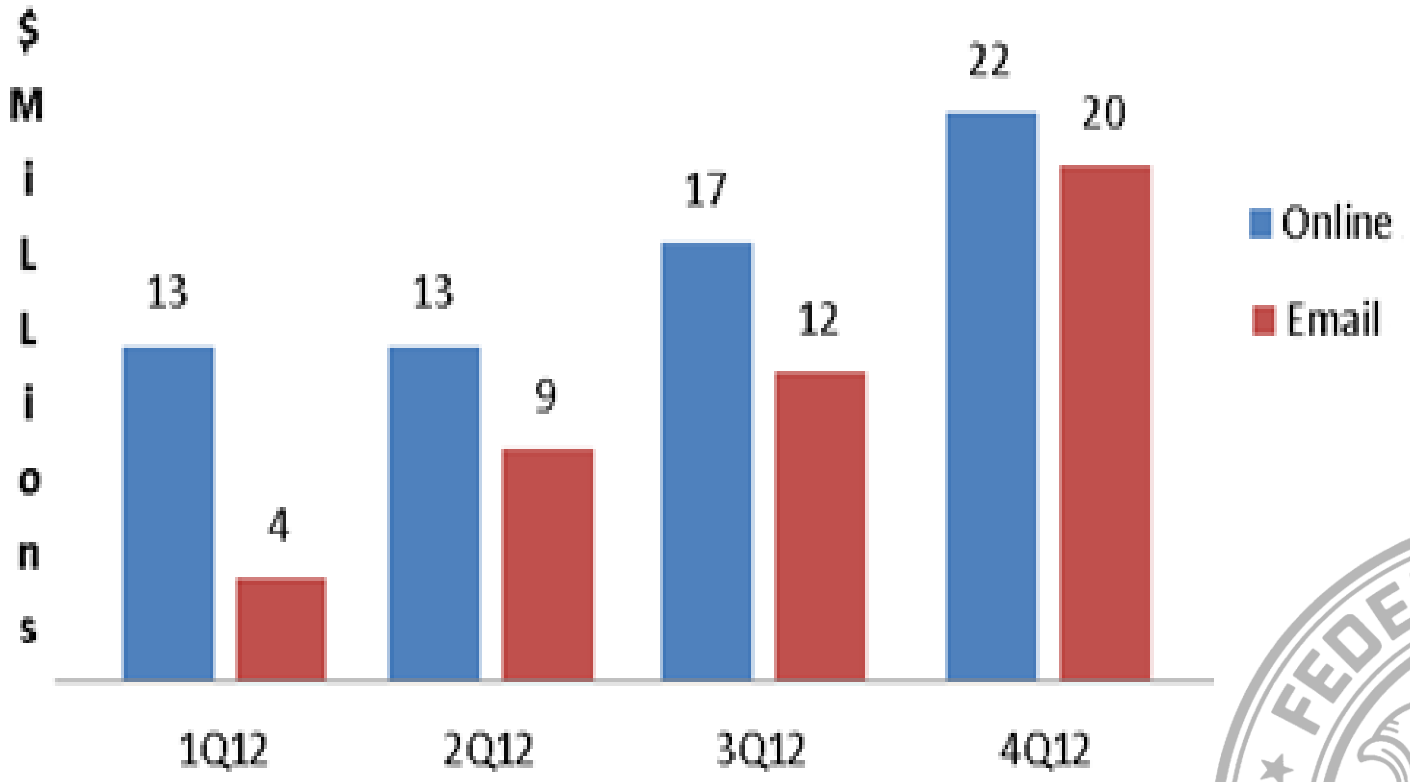
* The Texas Bankers Electronic Crimes Task Force

Commercial Account Takeover Lawsuits

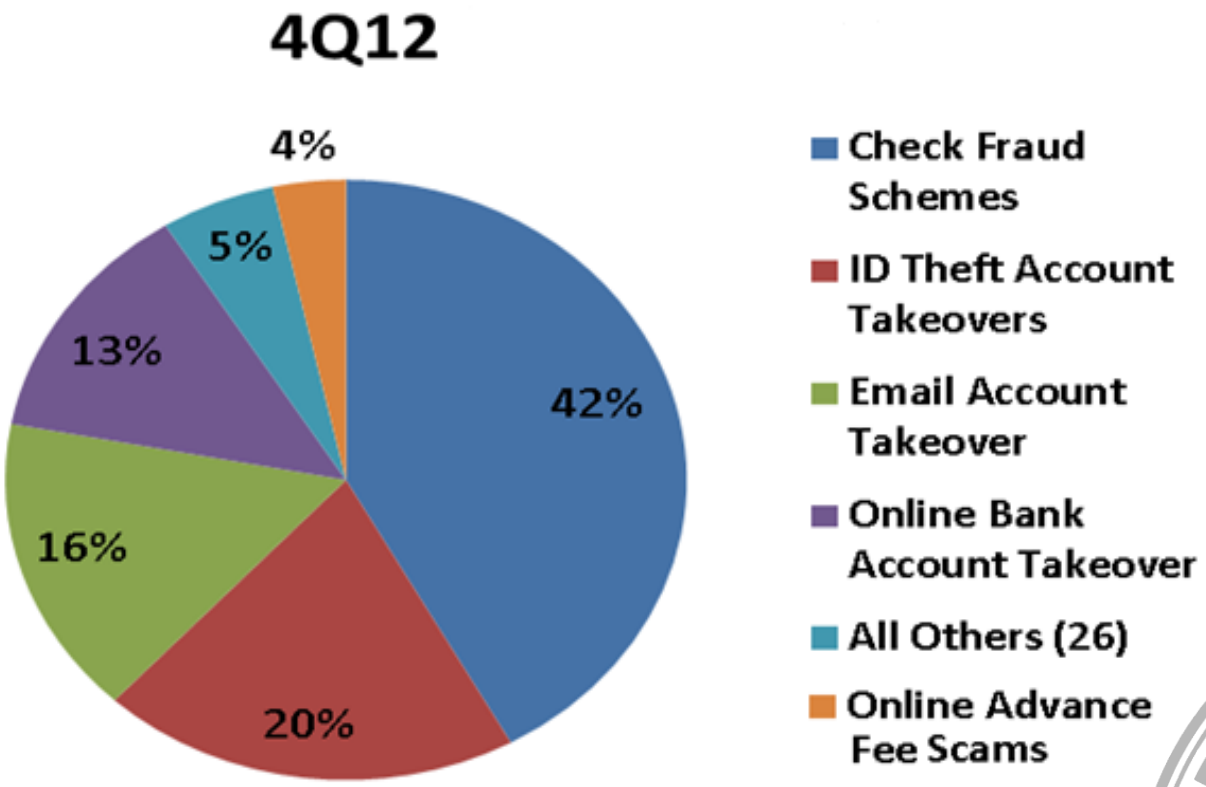
Patco: In 2009, cyber criminals gained control of Patco's internet banking account and transferred $600,000 out of the account via ACH. The bank recovered $250,000, but held Patco liable for the $350,000 that could not be recovered. Patco sued the bank in federal district court to recover the funds and lost. However, in 2012, the First Circuit Court of Appeals reversed the district court's finding of summary judgment in favor of the bank. The appeals court found that 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. The Appeals Court sent the case back to the District Court for further proceedings consistent with its opinion that the bank's security system was not commercially reasonable.

Experi-Metal: During a six hour period, after obtaining the company's login credentials using a phishing attack, cyber criminals initiated 93 fraudulent ACH transactions totaling $1.9 million. The bank was able to recover all but $560,000 and held Experi-Metal liable for the loss. The company sued the bank in federal district court and won in a decision that was announced in June 2011. 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.

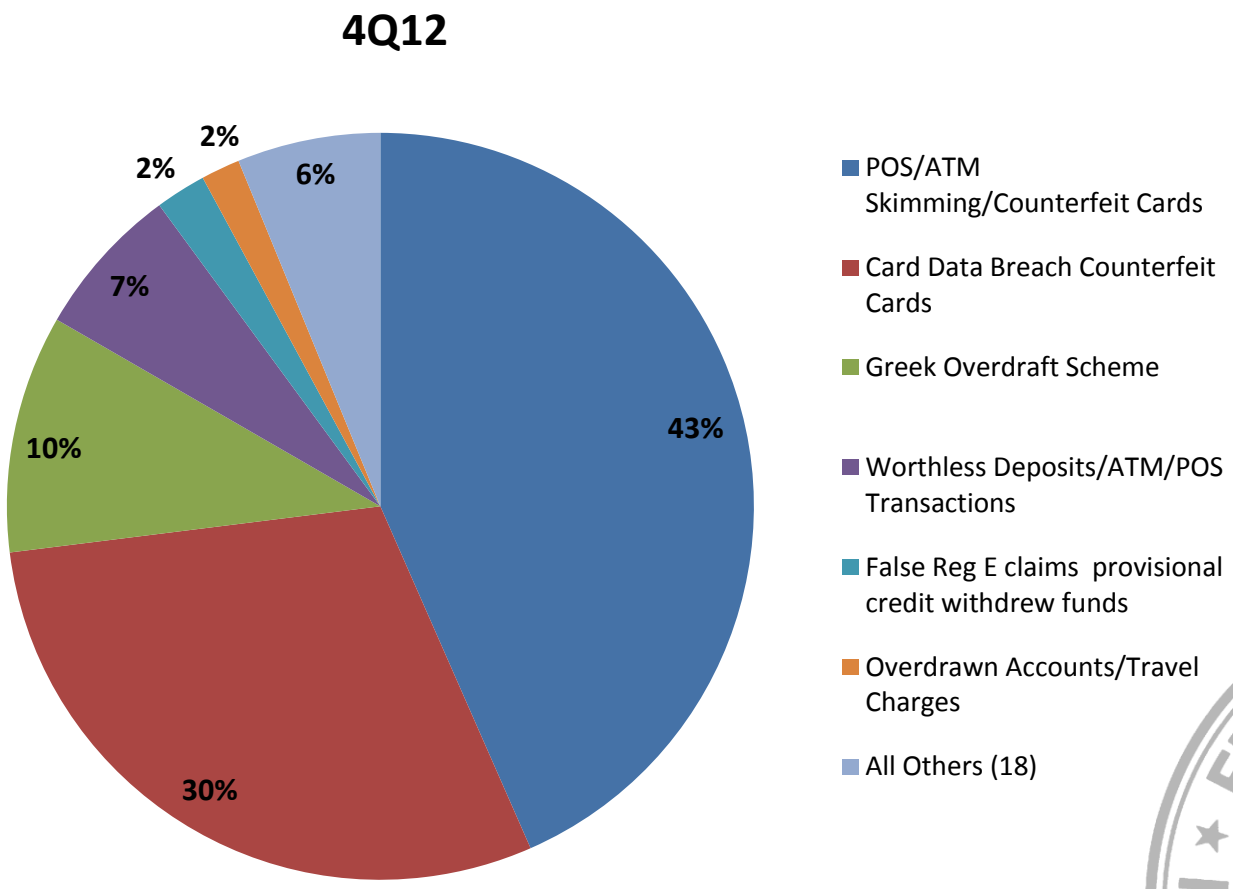
Online vs Email Account Takeover



Wire Losses by Fraud Type

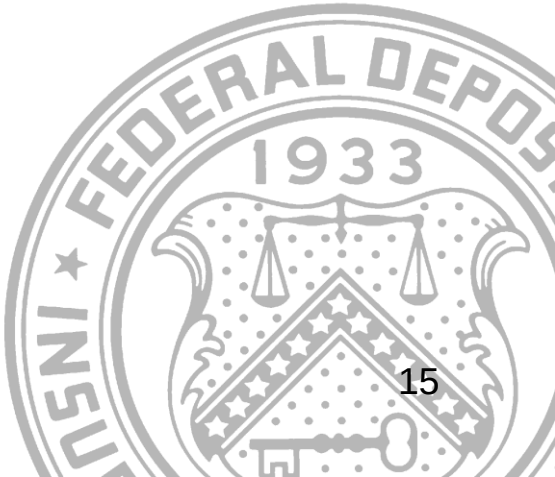


Debit Card Losses by Fraud Type

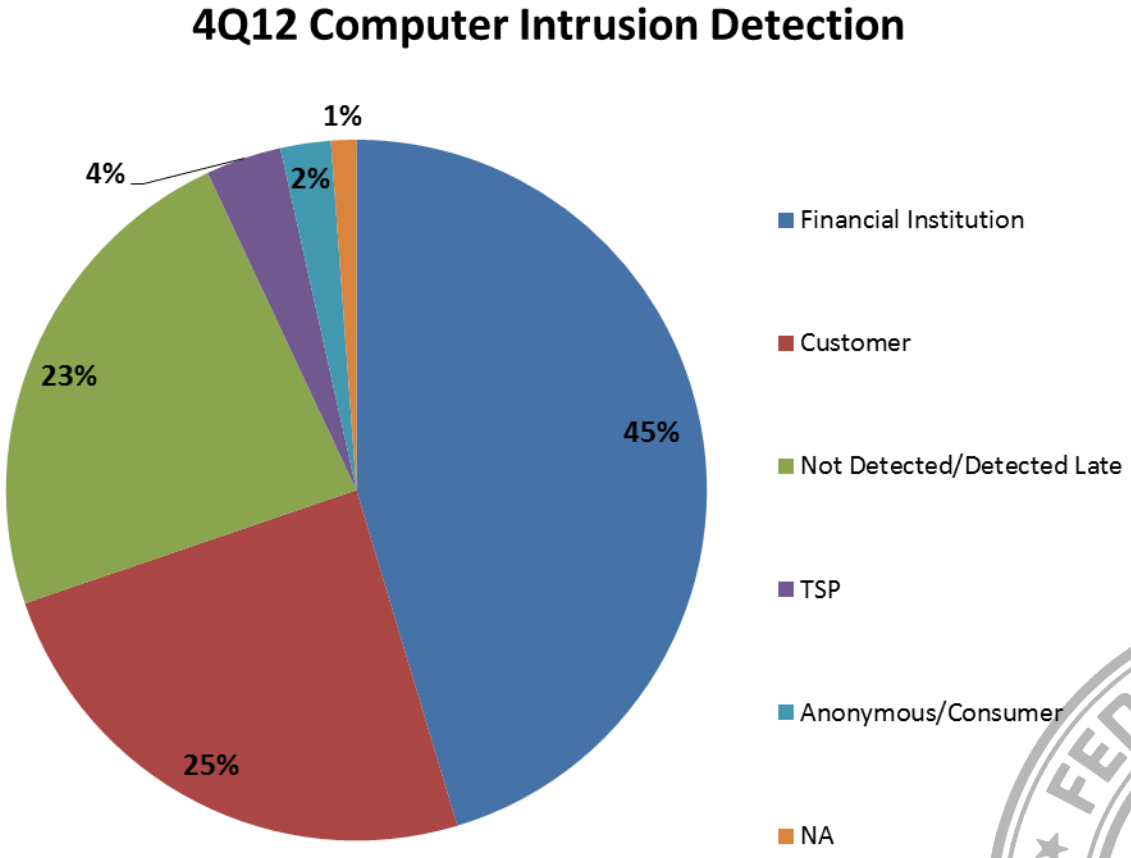


Mitigating Fraud/Abuse

Maintain an <u>EFFECTIVE</u> Information Security Program



Detection


4Q12 Computer Intrusion Detection
1%
4%
2%
23%
45%
25%
Financial Institution
Customer
Not Detected/Detected Late
TSP
Anonymous/Consumer
NA

Risk Mitigation Practices/Controls

- Update your risk assessment
- Have comprehensive written policies and procedures
- Utilize security features built into your systems
- Deploy robust multifactor authentication solutions
- Limit administrative rights on workstations
- Deploy other security controls (e.g. firewalls, IDS, antivirus, etc...)

Risk Mitigation Practices/Controls

- Implement appropriate employee separation-of-duties
- Review security, maintenance, and activity logs/reports
- Use AML/BSA Account Monitoring Tools
- Implement an effective audit program
- Train employees

Mitigation (continued)

- Know your customers:
  - Existing relationship experience
  - Require customers to complete applications
  - Understand customer's industry and specific financial trends
  - Visit customers site
  - Ensure customer systems are reasonably secure
- Establish comprehensive contracts and agreements
- Consider using prefunding or reserve arrangements
- Understand customer file submission timeframes and scrutinize those files that fall outside of traditional patterns
- Establish reasonable file 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 (e.g. daily)
  - Report suspicious activity to the bank and police
  - Protect passwords

- Business Continuity and Disaster Recovery Incident Response
  - Act immediately when unauthorized transactions are identified
  - Notify your primary regulatory agency when a compromise occurs
  - File suspicious activity reports

Vulnerabilities vs Remedies
No silver bullet

- Identify main vulnerabilities
  - Endpoints (USB, web, perimeter, remote access)
  - Servers (applications)
  - CS (control systems with legacy options)
  - **Users**

Vulnerabilities vs Remedies
No silver bullet

- COUNTER WITH:
  - Secure configurations & monitoring
  - Patching & VERIFICATION
  - Maintaining a baseline configuration – change management
  - Account management (user accounts not business accounts)
  - User awareness training!! (again and again)

"Automating a bad process just leads to getting bad results more quickly"

Denial of Service

A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**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 DoS are:

- A particular web or e-mail resource becoming unavailable
- Slow network performance
- Inability to access some network resources

Social Media

Flash Mob Attacks – usually involve a large group of unassociated people that are organized via mass communication campaigns to perform a group act in public.

Best Practices

Assess your organization's risk for a DoS. If your organization relies heavily on web-based services consider the potential impact to your operations if hit by a DoS and develop an appropriate mitigation plan.

Develop a checklist of actions to take in the event of a DoS and have contact information for your Internet Service Provider ISP and your web hosting providers readily available. If you use a web host for your services, be familiar with their DoS mitigation policies and plans.

Be familiar with the services your ISP might offer to mitigate a DoS, such as temporarily increasing your bandwidth, switching your IP address, and blocking attacking IP addresses.

Best Practices (Cont.)

Understand your normal amounts of daily network traffic as well as the performance of your system. Many DoS attacks may not bring the site down but can significantly reduce service. Properly configured performance monitoring can be a major help in detecting an attack early.

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

Review US-CERT cyber security tip “Understanding Distributed-Denial-of-Service Attacks”

Thank You!

James Brignac

IT Examination Specialist

FDIC Dallas Regional Office

JBrignac@FDIC.GOV

Marvin McCoy

IT Examination Specialist

FDIC Memphis Area Office

MMcCoy@FDIC.GOV

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)

References

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)

Texas Bankers Electronic Crimes Task Force

PCI Security Standards Council

US CERT

Sources

Federal Deposit Insurance Corporation (2013, March 21). *Cyber Fraud and Financial Crimes Report as of December 31, 2012*. Division of Risk Management Supervision.

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-pacto-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

Lardinois, F. (2012, May 23). McAfee: Mobile Malware Explodes, Increases 1,200% In Q1 2012. *TechCrunch.com.* Retrieved April 26, 2013, from http://techcrunch.com/2012/05/23/mcafee-mobile-malware-explodes-increases-1200-in-q1-2012/

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

Zetter, K. (2011, April 20). Top Federal Lab Hacked in Spear-Phishing Attack. *Wired.com*. Retrieved April 26, 2013, from http://www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack/