



Managing Emerging Technology Risk

Federal Deposit Insurance Corporation

New York Regional Office

May 16, 2012





Managing Emerging Technology Risk

- Regulatory guidance and best practices for managing risks pertaining to:
 - payment systems,
 - social media sites,
 - mobile banking, and
 - virtualization/cloud computing
- Security and data integrity challenges in safeguarding customer information



Payment Systems

Non-Cash Payment Systems in the US:

- Check Clearing Systems
- Automated Clearing House (ACH) Systems
- Card-based Credit/Debit (e.g., Amex, Discover, MasterCard, Visa, etc.)
- Prepaid/Stored Value Card Programs
- Electronic Funds Transfer Networks (e.g., Star, Cirrus, Pulse, etc.)
- Person-to-Person or P2P (e.g., PayPal, etc.)



Payment Systems

Payments risk covers all FDIC supervisory disciplines:

- Safety & Soundness
- Compliance/Consumer Protection
- Bank Secrecy Act / Anti-Money Laundering
- Technology/Operations



Corporate Account Takeover

Corporate accounts are targeted because of the large balances **and** the ACH credits that are generated have expedited funds availability.



Corporate 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



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.



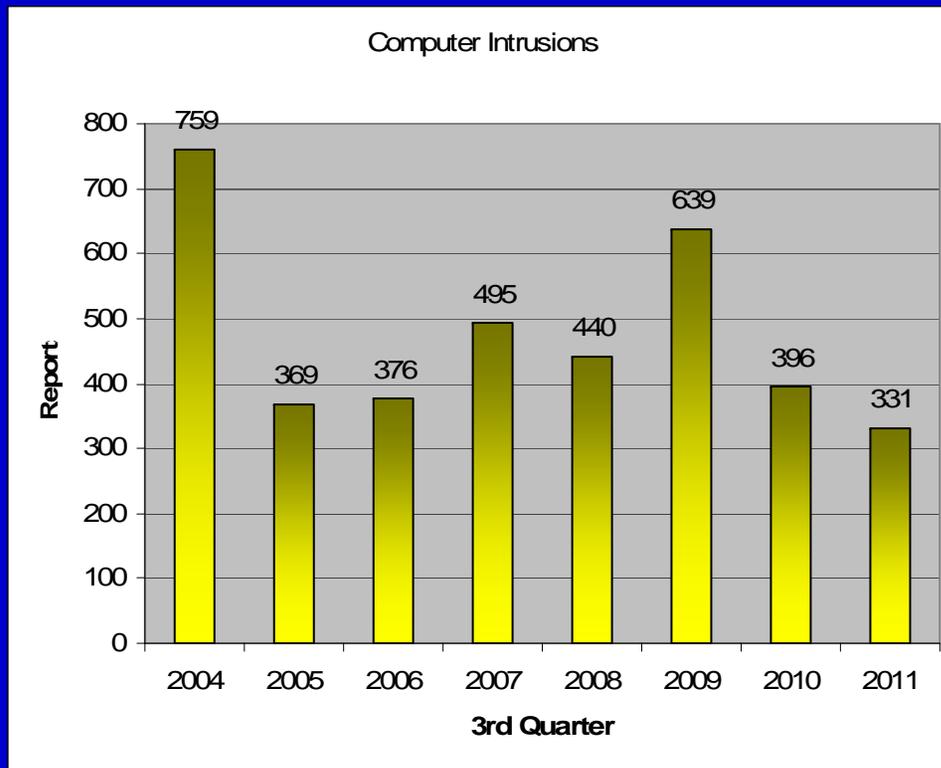
Cyber Fraud and Financial Crime Reports

**FDIC Division of Risk Management
Supervision**

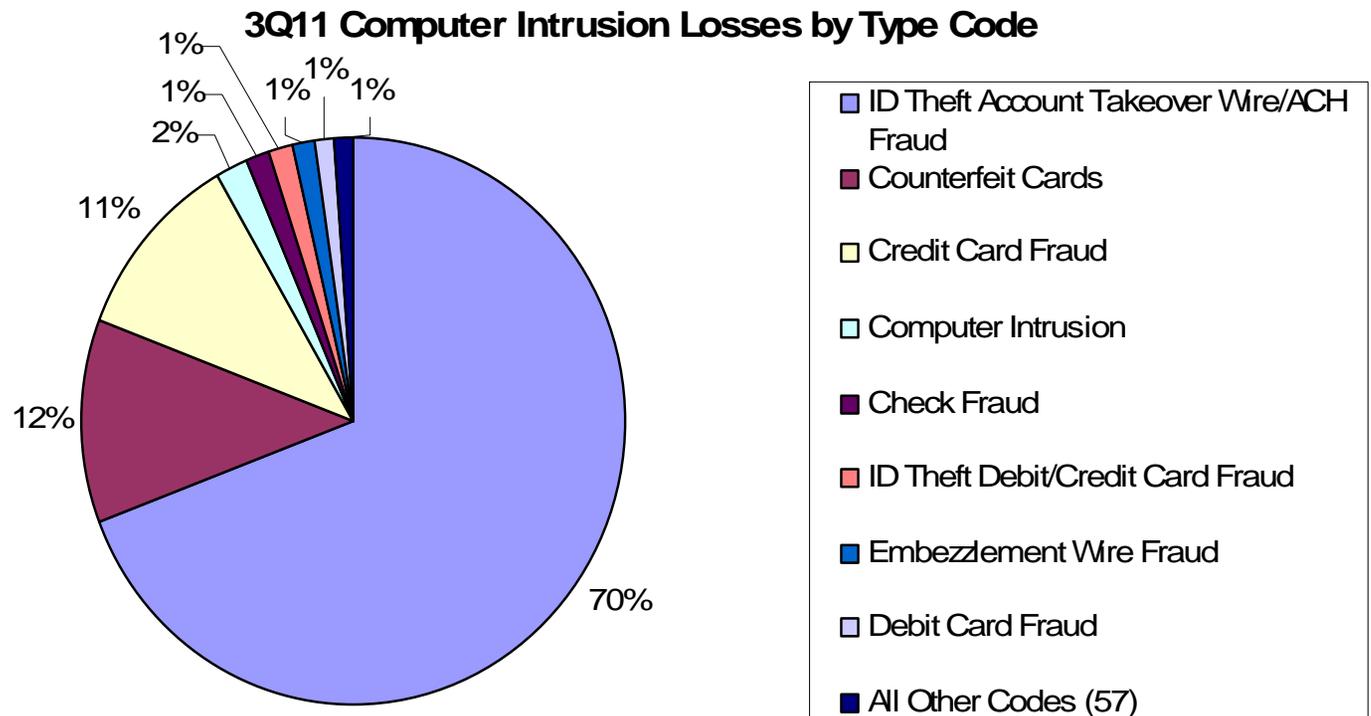
**Technology Supervision Branch
Cyber Fraud and Financial Crimes Section**

Computer Intrusions

3rd Quarter 2011

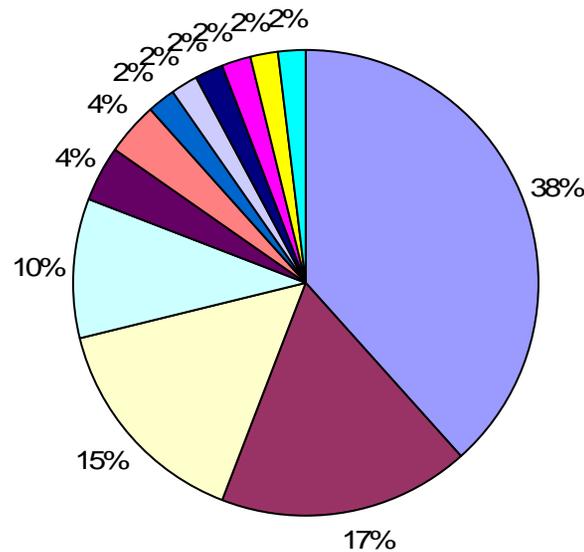


Computer Intrusion Losses by Type Code 3rd Quarter 2011



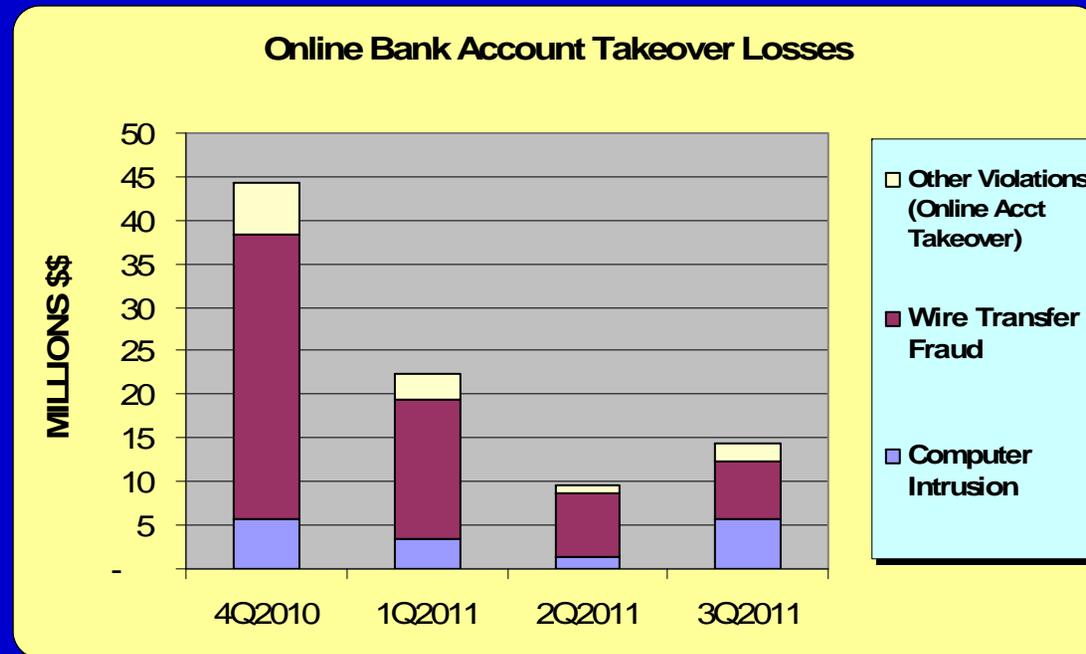
Computer intrusion detection rates 3rd Quarter 2011

Computer Intrusion Detection 3Q11



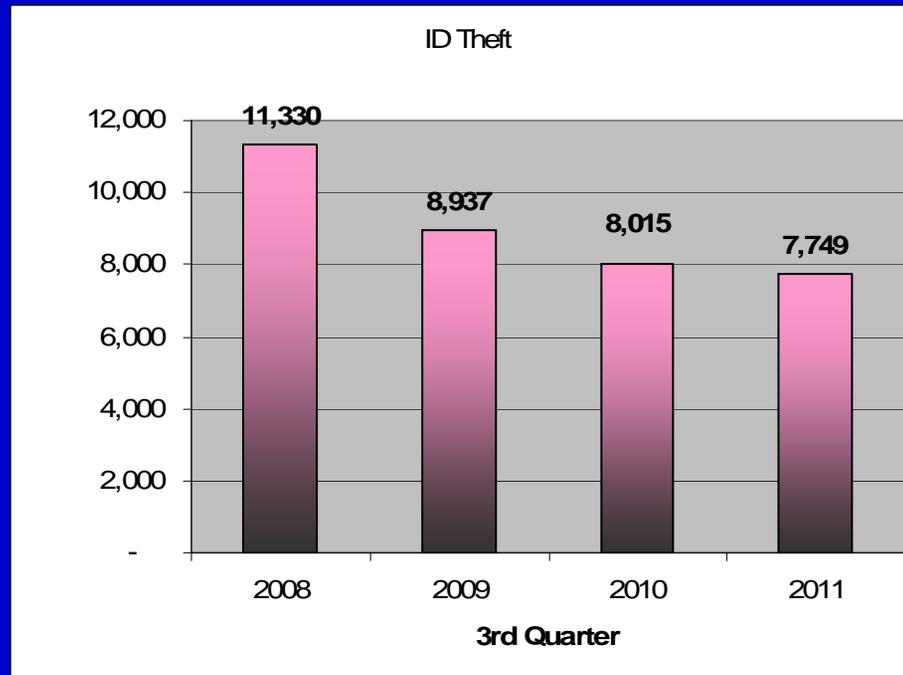
- Customer Notified Bank
- FI Employees
- Not Detected
- Card Network/Payment Processor
- RDFI
- IRC - Employee Acct Reviews
- Money Mules Notified
- Western Union
- Returned Wire Notice
- Notified by a Reporter
- University Detected
- TSP Detected Bad IP

Online bank account takeovers 3rd Quarter 2011



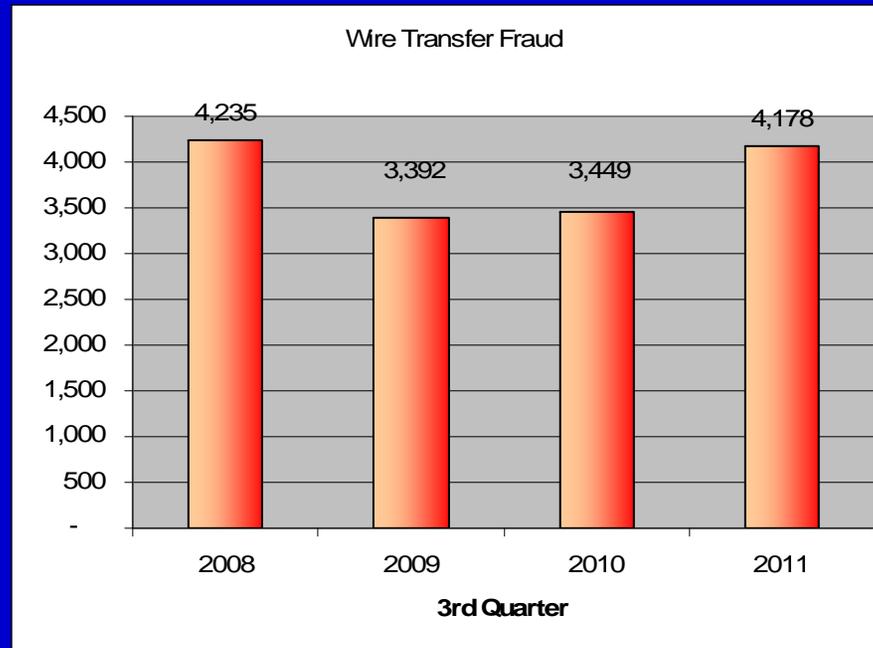
ID Theft reports

3rd Quarter 2011



Wire transfer fraud reports

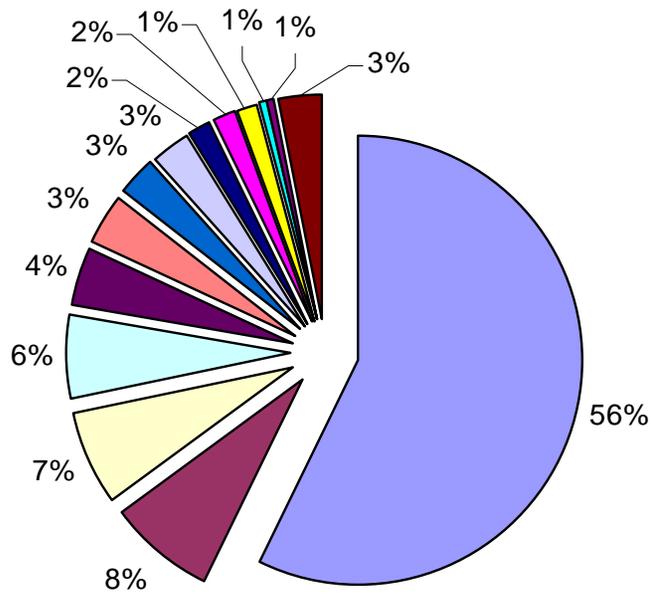
3rd Quarter 2011



Wire Transfer Fraud Losses

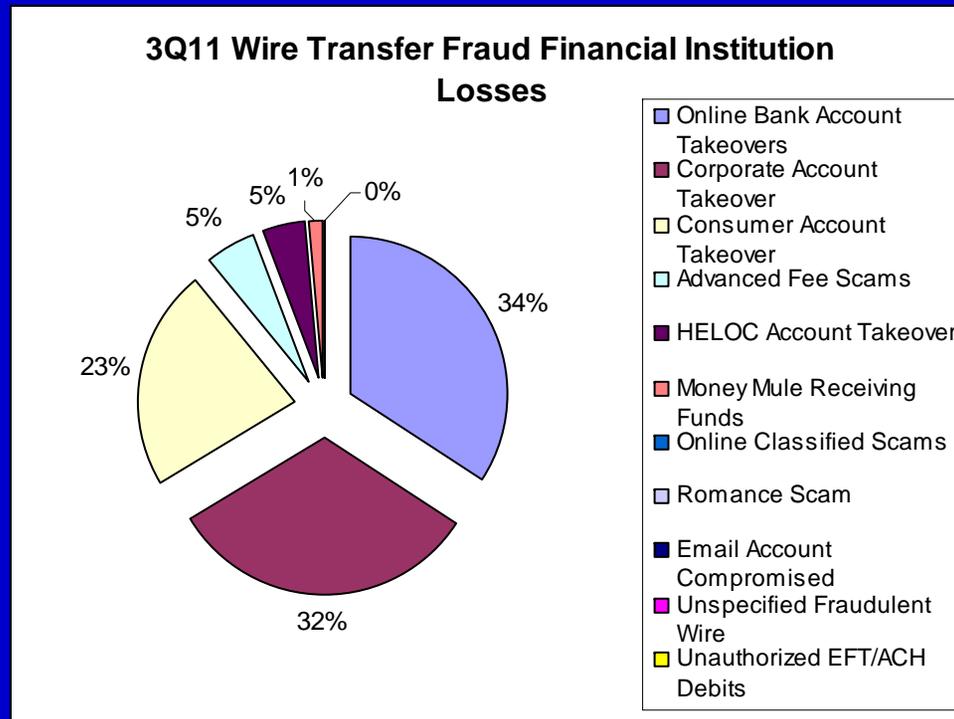
3rd Quarter 2011

Wire Transfer Fraud 3Q11 Losses



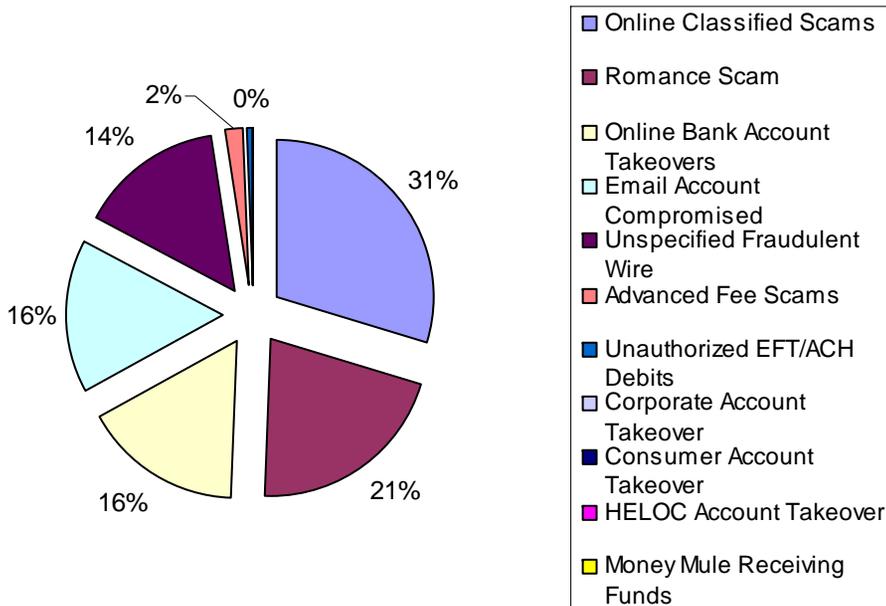
- Mortgage Fraud
- Credit Card Fraud
- Commercial Loan Fraud
- Wire Transfer
- ID Theft
- Counterfeit Checks
- Check Fraud
- Online Banking
- Terrorist Financing/Money Laundering
- Consumer Loan
- Computer Intrusion
- Insider Fraud
- Telephone Fraud
- All Other (834)

Wire Transfer Fraud Financial Institution Losses 3rd Quarter 2011

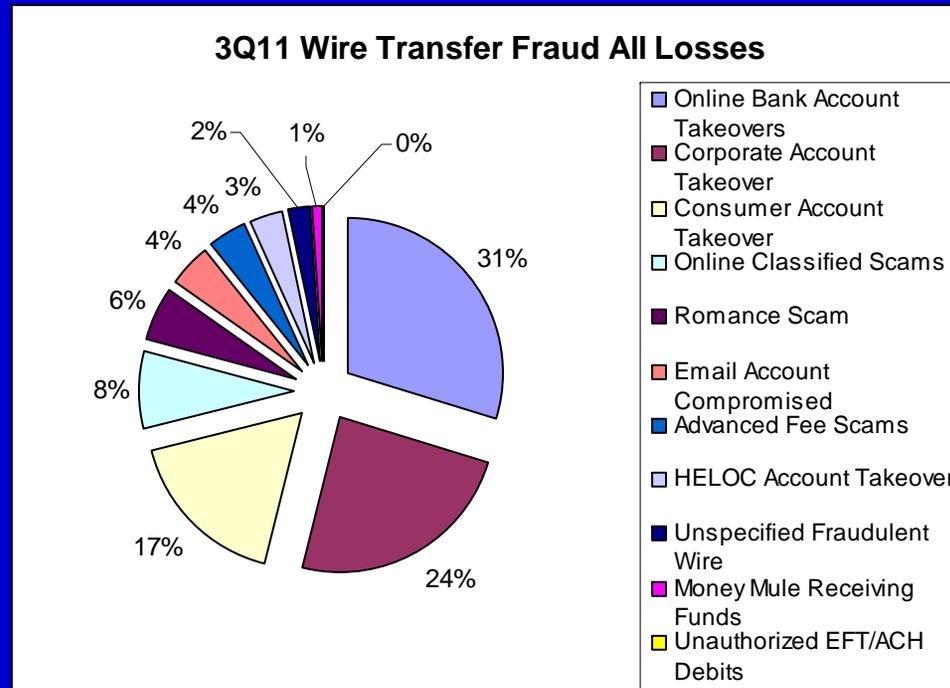


Wire Transfer Fraud Customer Losses 3rd Quarter 2011

3Q11 Wire Transfer Fraud Customer Losses



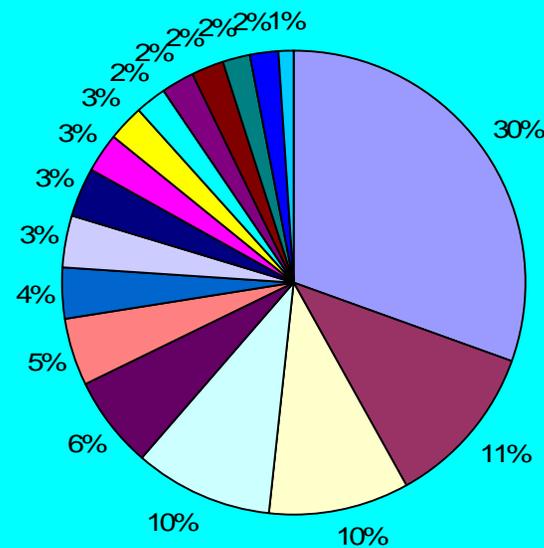
Wire Transfer Fraud All Losses 3rd Quarter 2011



Wire Fraud Loss- Ingress Channel

3rd Quarter 2011

3Q11 Wire Fraud Loss - Ingress Channel



- Email
- Online Classifieds/Auction
- Branch
- Phishing/Malware
- German/US IPS
- Unknown
- Email (originating from Malaysia)
- UPS Letter
- ID Theft/Account Takeover
- Logged on from Local IP
- Logged on from Customer's PC
- Logged in from US IP
- Logged in from Korea
- FAX
- Telephone Transfer
- Mobile Device (Malaysia provider)
- Other (11)
- Other (1)

Debit Card Fraud

➤ Volume

➤ Means of Exploitation





Risk Mitigation Practices/Controls

- Utilize multi-factor authentication
- Install and regularly update firewalls, malware/spyware protection, and commercial anti-virus software
- Initiate payments under dual control



Risk Mitigation Practices/Controls

- Limit administrative rights on workstations
- Encourage corporate clients to reconcile their bank accounts daily
- Use AML/BSA Acct Monitoring Tools
- Customer (Public) Awareness and Education and Employee Training



Information Technology (IT) Examinations

IT examinations address a wide range of data security issues such as:

- Information security programs and compliance with Gramm-Leach-Bliley Act, Sect. 501(b) requirements;
- Business continuity planning and physical security;
- IT audit coverage and independent review of controls;
- IT security strategies and policies and personnel controls



Primary Supervisory Examination Issues

Primary supervisory examination issues continue
in the areas of :

- Gramm-Leach-Bliley Act (GLBA) compliance
- Vendor Management programs
- Business Continuity/Disaster Recovery planning
- IT Audit Coverage
- Network/access controls



Mobile Device Fraud

- Fraudulent Wire Transfer
- Exploitation Methods
- Risk Assessment

The image shows a vertical strip on the left side of the slide. It features a textured, metallic background with embossed symbols: a pair of scales of justice at the top, a key in the middle, and the letters 'FDIC' at the bottom. The background also has a repeating pattern of small, stylized 'U' shapes.

Social Media Sites

- Security Risks
- Reputation Risk
- Corporate Governance
- Resources

Cloud Services

- Risk Assessment Issues
 - Governance
 - Strategic Considerations
 - Policies
 - Topology
 - Controls
 - Contracts/Agreements
 - Audit





Examination/Financial Institution Guidance

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 Retail Payment Systems Handbook (FIL-6-2010)

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

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

FDIC Supervisory Insights Journal (Quarterly)



Examination/Financial Institution Guidance (Continued)

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

Special Alert SA-147-2009: *Fraudulent Electronic Funds Transfers*
(August 2009)

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

National Institute of Standards & Technology (NIST)

Trade Associations (ABA, BITS)

PCI Security Standards Council

US CERT

Thank you!



Contact Information

Stephanie Williams
Examination Specialist
(Information Technology)
New York Regional Office
SteWilliams@fdic.gov

Gerald Suslak
Examination Specialist
(Information Technology)
New York Regional Office
GSuslak@fdic.gov

Robert Sargent
Examination Specialist
(Information Technology)
Boston Area Office
RSargent@fdic.gov