CURRENT TRENDS IN FINANCIAL INSTITUTION FRAUD

WITH MIKE THOMAS
PARTNER, CROWE HORWATH LLP

January 10, 2013
Agenda

- Fraud Statistics
- Internal Fraud Red Flags
- Recent Fraud Schemes
FRAUD STATISTICS
Impact of Fraud on Financial Institutions

• Hard to measure
• No one universal definition of fraud = various interpretations
• No one agency that is responsible for investigating fraud
• Additionally, many fraud losses are misreported
• Why does this occur?
  – Because most institutions don’t recognize when a fraud has occurred and chalk it up to a bad underwriting decision or another form of operational expense.
Cost of Fraud

• Other less-quantifiable costs of fraud to the organization:
  – Reputation risk to financial institution
    • Customers trust us with one of their most significant possessions: Their money
    • Reputation risk is difficult to quantify
  – Increased regulatory focus
  – Morale impact on employees
Suspicious Activity Reports

• The Bank Secrecy Act (BSA)

• Regulations require that financial institutions file Suspicious Activity Reports (SARs)
  – Report known or suspected violations of law or suspicious activity
  – Filed with the Department of Treasury’s Financial Crimes Enforcement Network (FinCEN)
Suspicious Activity Reports

• FinCEN compiles statistics based on the filed SARs to identify trends and patterns for use by not only the financial institutions but also by law enforcement

• Multiple types of financial institutions are required to file SARs:
  – Depository Institutions
  – Money Service Businesses
  – Securities Sector
  – Others
## Suspicious Activity Reports

### SAR Data from 2001 thru 2011

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Depository Institutions</td>
<td>203,538</td>
<td>273,823</td>
<td>288,343</td>
<td>381,671</td>
<td>522,655</td>
<td>567,080</td>
<td>649,176</td>
<td>732,563</td>
<td>720,309</td>
<td>697,389</td>
<td>794,710</td>
</tr>
<tr>
<td>Money Services Business</td>
<td>5,723</td>
<td>209,512</td>
<td>296,284</td>
<td>383,567</td>
<td>496,400</td>
<td>578,439</td>
<td>531,761</td>
<td>530,518</td>
<td>596,494</td>
<td>673,531</td>
<td></td>
</tr>
<tr>
<td>Casinos and Card Clubs</td>
<td>1,377</td>
<td>1,827</td>
<td>5,095</td>
<td>5,754</td>
<td>6,072</td>
<td>7,285</td>
<td>9,943</td>
<td>11,162</td>
<td>12,093</td>
<td>13,987</td>
<td>17,627</td>
</tr>
<tr>
<td>Securities and Futures Industries</td>
<td>4,267</td>
<td>5,705</td>
<td>6,936</td>
<td>8,129</td>
<td>12,881</td>
<td>15,104</td>
<td>18,385</td>
<td>18,758</td>
<td>19,955</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subtotal</td>
<td>204,915</td>
<td>281,373</td>
<td>507,217</td>
<td>689,414</td>
<td>919,230</td>
<td>1,078,894</td>
<td>1,250,439</td>
<td>1,290,590</td>
<td>1,281,305</td>
<td>1,326,628</td>
<td>1,505,823</td>
</tr>
</tbody>
</table>

Source: Financial Crimes Enforcement Network (FinCen)
Of all SARs filed since 2001, 84% of the total were filed since 2005.

Source: Financial Crimes Enforcement Network (FinCen)
Suspicious Activity Reports

Suspicious Activity Report Filings by Depository Institutions and Non-Depository Institutions*
For the Period January 1, 2007 through December 31, 2011

2007: 649,176
2008: 732,563
2009: 720,309
2010: 697,389
2011: 794,710

* Non-depository institutions consist of the money services business; securities and futures industries; and casino and card clubs.
Suspicious Activity Reports

Significant Observations from 2011

- 10 of 21 reportable suspicious activity categories saw increases in CY2011
  - Increases ranged from a high of 127% to less than 1%

- In 2011, the summary characterization BSA/Structuring/Money Laundering showed an increase of approximately 15%
  - Compared to the prior reporting period for this category

- Reports of Terrorist Financing declined 14%
  - From 711 instances in 2010 to 609 for the same period in 2011

- Though having experienced decreases in 2009 and 2010, the number of reports indicating Consumer Loan Fraud (in whole or part) significantly rose in 2011, up 127% from the prior year

Source: Financial Crimes Enforcement Network (FinCen)
Suspicious Activity Reports

Significant Observations from 2011

• The number of depository institution SARs identifying **Mortgage Loan Fraud as a Characterization of Suspicious Activity** continued to rise (up 30.6% in calendar year 2011)

• Quite markedly, Mortgage Loan Fraud is the only summary characterization that has experienced an increase every year since 1996
  – The past two years (2010 and 2011) account for nearly 37% of all noted instances of this specific activity for the last decade

• **Note that depository institutions may submit Mortgage Loan Fraud SARs well past the actual date of the activity**

• This upward spike in mortgage fraud counts is in predominant part attributable to **mortgage repurchase demands** and special filings generated by several institutions

Source: Financial Crimes Enforcement Network (FinCen)
Suspicious Activity Reports

Significant Observations from 2011

• SARs indicating **National Credit Union Administration (NCUA)** as the Primary Federal Regulator continued to rise
  – **Up 6%** in 2011 from the previous twelve months
  – This increase represents a continued trend upward for the NCUA, the only federal regulator that has shown an increase **every year since 1998**

• Fraud-related activities (Check Fraud, Commercial Loan Fraud, Consumer Loan Fraud, Credit Card Fraud, Debit Card Fraud, Mortgage Loan Fraud, and Wire Transfer Fraud) **accounted for 27% of suspicious activities reported by depository institutions in 2011**
  – **This represents a slight increase** in the number of instances reported (in whole or part) for fraud-related activities, as a group, for the same period in 2010

Source: Financial Crimes Enforcement Network (FinCen)
Suspicious Activity Reports

Significant Observations from 2011

• The volume of SAR filings in 2011 represented a high over any previous calendar year
  – Increased 14% these last twelve months
• Reports of Wire Transfer Fraud increased 9% in the last twelve months
• Depository institution SARs listing Mysterious Disappearance jumped 35%
  – Noticeable contrast to the prior year of filing which saw a decrease of 16% for the same summary characterization
• The number of depository institution SARs where the filer indicated Counterfeit Credit/Debit Card as a characterization rose 39%
  – Comparing 2011 to the previous year

Source: Financial Crimes Enforcement Network (FinCen)
Poll #1

What is the only fraud summary characterization that has experienced an increase every year since 1996?

a) Check Fraud  
b) Mortgage Fraud  
c) Terrorist Financing  
d) Wire Transfer Fraud
Poll #1

Answer

b) Mortgage Fraud
INTERNAL FRAUD RED FLAGS
Fraud “Red Flags”

- Unusually high personal debts
- Living beyond one’s means
- Excessive gambling habits
- Alcohol problems
- Drug problems
- Feeling of being underpaid
- Feeling of insufficient recognition for job performance
- Poor credit rating
Fraud “Red Flags”

• Consistent rationalization of poor performance
• Wheeler-dealer attitude
• Intellectual challenge to “beat the system”
• Criminal record
• Not taking vacations of more than two or three days
• A department that lacks competent personnel
• A department that does not enforce proper procedures for authorization of transactions
• No separation of duties between the accounting functions
Fraud “Red Flags”

- No explicit and uniform personnel policies
- Inadequate attention to details
- Placing too much trust in key employees
- Pay levels not commensurate with the level of responsibility assigned
- Failure to discipline violators of company policy
- Not adequately checking background before employment
Poll #2

Which of the following are Internal Fraud Red Flags?

a) Excessive gambling habits
b) Unusually high personal debts
c) Not taking vacations of more than two or three days
d) All of the above
Poll #2

Answer

d) All of the above
RECENT FRAUD SCHEMES
Within the last several months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium businesses, municipal governments, and school districts.

In a typical scenario, the targeted entity receives a “spear phishing” e-mail which either contains an infected attachment, or directs the recipient to an infected website. Once the recipient opens the attachment or visits the website, malware is installed on their computer. The malware contains a key logger which will harvest each recipient’s business or corporate bank account login information.

Shortly thereafter, the perpetrator either creates another user account with the stolen login information or directly initiates funds transfers by masquerading as the legitimate user. These transfers have occurred as both traditional wire transfers and as ACH transfers.
Fraudulent ACH Case Study

- A bank customer's laptop was hacked into.
- The person at the customer who inputs ACH transactions happened to look at her queue and noticed a $47,000 ACH for payroll that she had not input.
  - She cancelled the transaction before it processed, so the fraud did not occur.
- The customer called the bank and was advised to have all of their computers scanned by their IT person.
- The customer did so and found numerous computers/laptops had viruses including the virus that copies password information (including answers to security questions).
- The customer has since cleaned their computers and installed virus protection software.
Fraudulent Wire Case Study

• A loan assistant received an email from a customer, responded to the email, but forgot to attach the document the customer requested.
• She called him and apologized for not attaching the information.
  – The customer had no idea what she was talking about (he had not sent the email).
• A few days later, an email wire request for this customer came through.
  – The loan assistant called the customer immediately to ask if he had made the request.
  – He had not, so she did not process it.
• The email had the request and a facsimile signature saved in the signature matched the customer's identically.
• Somehow the fraudster had hacked into the customer's email and was able to send emails from their account as well as obtained bank employee names and email addresses.
Fraudulent Wire Case Study

• A bank suffered a $180,000 loss due to a wire fraud
• The wire request was made over the phone to the Central Wire Desk and was covered by a Wire Agreement that includes unique PIN codes, Call-Back procedures, and recorded lines
• The fraudster had both the unique PIN codes and had the call-back number re-routed (via the phone company) to his cell-phone
  – Note that the wire clerk followed all procedures correctly
• The customer had lost their work laptop which included all the wire information (call-back number and PIN)
Fraudulent Electronic Funds Transfers – Prevention Techniques

• Basic Internal Controls:
  – Customer Verifications (ex. call-backs)
  – Scheduled Transfers

• There are several technology solutions that help banks determine when multiple parties are “on-line” at the same time. Also, “smart systems” are available to look at customer trends/patterns and will highlight unusual activity.

• Increased customer awareness and preventative techniques (security protocols, encryption, malware software, etc.).
Recent Fraud Schemes

Teller Cash Fraud

• A head teller stole over $7 million in cash from the cash vault at a $52-million credit union, forcing regulators to liquidate the 70-year-old institution
• The teller confessed to stealing the money by walking out of work on a weekly basis with stacks of $100 bills, sometimes containing as much as $100,000
• The teller was able to hide her thefts by making journal entries into the vault cash account whenever there was an audit or cash count by the credit union supervisory committee, and then making adjusted entries after those counts were completed
Recent Fraud Schemes

Teller Cash Fraud (Updated)

- The teller was sentenced to eight years and eight months in prison and ordered to repay the stolen funds, but that is unlikely because she gambled them all away on Ohio River casino boats.
- She stole $7 million over 46 months, a total of about $150,000 every month, or about $37,000 every week.
- A bond company paid $2 million of the loss, but about $5 million had to be written off as an expense.
- The theft bankrupted the $52 million credit union, forcing it to merge with a larger credit union last July.
Teller Cash Fraud
– Preventative Techniques

 Surprise Cash Counts

• Include all cash supplies and cash items (returned checks, food stamps, redeemed bonds, etc.) assigned to the teller
• Physically count each bill in the teller’s possession
  – For Vault Tellers, physically count all loose bills and large bills ($50s and $100s); sample count strapped $20s, $10s, $5s and $1s (“fan” straps not counted)
  – For any currency in “Fed wrapped” packages, open packages and “fan” bills to ensure legitimacy
  – For bagged shipments, either verify or control until pick-up and positively confirm with receiver
  – For bagged coin, “feel” contents (e.g. pennies are smaller than quarters) and verify on a sample basis
• Balance cash counted back to the general ledger (i.e. the last time the teller actually balanced to the general ledger)
Teller Cash Fraud – Preventative Techniques (continued)

• If the teller was counted at any time subsequent to teller balancing (e.g., the teller balanced to the general ledger at 2pm, but the count was performed at 4pm), physically verify and control any post cut-off work (e.g. actual cash ins and cash outs)
  – Do not rely on teller tape/machine totals, as these can be easily misrepresented

• On the day following the cash count, ensure Teller Balancing did not make any adjustments to the teller’s general ledger cash balance
  – If so, the individual responsible for performing the surprise cash count should investigate for propriety

• On the day following the cash count, ensure there are no outstanding “Cash in Transit” on the general ledger for the teller
  – If there are, follow to ensure propriety
Recent Fraud Schemes

Certificates of Deposit Fraud

- A former branch manager for an Iowa Bank pleaded guilty last week to selling more than $4 million of phony certificates of deposit to banks, credit unions and other entities, and now the buyers are trying to get their money back.

- A N.H. Credit Union, which bought a $99,000 CD it thought was issued by the Iowa Bank, is one of about 50 institutions victimized in the scam, which ran between 1995 and 2008.
  - The credit union has filed a civil suit against the $890 million-asset Iowa Bank.

- The former branch manager, who worked at the Iowa Bank for 28 years, confessed to selling the phony CDs, then using two bank accounts in the names of deceased bank customers to launder the proceeds from the scam.
MINNEAPOLIS—Yesterday, federal criminal charges were filed against a 47-year-old woman who was charged with one count of embezzlement by a bank officer for allegedly stealing hundreds of thousands of dollars from the CD accounts of customers at a Marshall, Minnesota bank where she worked.

The charges state that from 1998 through June of 2012, the bank officer embezzled the money for her personal use.

If convicted, the bank officer faces a potential maximum penalty of 30 years in prison.
Certificates of Deposit Fraud – Preventative Techniques

- Ensure the “vault supply” is maintained under dual control
- Ensure the “working supply” is locked in the vault at night
- Ensure the “working supply” is assigned to designated individual(s) for accountability (Note: Normally, CSRs keep the working supply)
- Someone independent of sales and custody (or dual control) daily/weekly verifies sold items from the working supply
- For book entry certificates, controls should be in place to ensure that receipts given to customers for purchased certificates are compared to the deposit subsystem
Poll #3

What is the most cash a teller can embezzle?

a) The approved amount in the teller drawer
b) The approved amount in the Main Vault
c) Any amount up to the total cash suspense tickets
d) Zero – A teller would never embezzle cash
Poll #3

Answer

c) Any amount up to the total cash suspense tickets
Recent Fraud Schemes

Credit Card Identity Theft

- Six servers at several Washington-area high-end restaurants stole credit card numbers from customers and ran up a $750,000 tab at stores like Gucci and Barney’s of New York

- In New Orleans, a waitress was charged with selling up to 50 customers’ credit card information
  - The waitress sold the numbers for $220 apiece to two men who provided her with a machine used to scan the credit cards

- A Buffalo, N.Y., man was convicted of hiring several cashiers at local restaurants and a department store to steal customers’ credit card information
Recent Fraud Schemes

Credit Card Identity Theft

• Barnes & Noble Inc. bookstores has informed federal law enforcement authorities that "a sophisticated criminal effort" has potentially exposed customers' credit and debit card information to hackers who tampered with PIN pad devices at 63 of its stores.

• The company's statement did not speculate on the number of potentially affected cardholders, but said it is working with issuers and payment card brands to identify accounts that may have been compromised to allow issuers to employ extra fraud security measures on potentially impacted accounts.
Recent Fraud Schemes

Identity Theft – Counterfeit Check Fraud

- On May 27, 2009, a group of 18 defendants were charged with operating an identity theft ring that used information obtained from tellers at New York City banks to generate counterfeit checks from hundreds of accounts.

- Prosecutors charged that from November 2007 until February 2009, the ring collected personal and bank account information belonging to 500 people by paying off bank tellers and also by buying copies of legitimate payroll checks.
  - Thousands of counterfeit checks were manufactured with the information.

- From a Bronx apartment known as “the Lab,” the leaders of the ring used specialized computer software, scanners, printers, check stock, magnetic ink, and company logos found on the Internet to produce the fake checks, which were cashed by “soldiers” enlisted for the scheme.
Identity Theft – Preventative Techniques

• Enhanced customer awareness and training

• Compliance with Section 114 (Red Flag Guidelines) and Section 315 (Reconciling Address Discrepancies) of the Fair and Accurate Credit Transaction Act (FACT Act)
  – Including monitoring of 26 known “red flags” grouped as follows:
    • Alerts, Notifications or Warnings from a Consumer Reporting Agency
    • Suspicious Documents
    • Suspicious Personal Identifying Information
    • Unusual Use of, or Suspicious Activity Related to, the Covered Account
    • Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor
Identity Theft – Preventative Techniques (continued)

- Multifactor Authentication - Using more than one of the following ways to confirm identity:
  - What you know (user ids, pin numbers, passwords)
  - What you have (card, token)
  - What you are (your fingerprint, retina pattern)
  - Shared Secret—Prompts a user to enter multiple pieces of information that only that user would know (e.g., mother's maiden name, last transaction amount, etc.)
  - GeoLocation—Confirming that the location from which the user authenticates is consistent with trends or other information on hand about the user
  - Related foot-printing techniques include checking time of day, computer or MAC Addresses, etc.
Recent Fraud Schemes

Fictitious General Ledger Entry

• The former operations manager and head teller were convicted of stealing almost $600,000 by crediting their own accounts from general ledger funds
• The 35-year-old former operations manager was sentenced to 12 months in prison and ordered to pay $395,000 in restitution
• Earlier, the former head teller pleaded guilty to embezzling $185,000
• Prosecutors said the employees had control over their own accounts and each woman stole the funds by depositing money from general ledger accounts into their own checking accounts
Recent Fraud Schemes

Fictitious General Ledger Entry – Wire Transfer

- The former senior VP and CFO has been being charged with embezzling more than $339,000
- Charges were filed against a 56 year old man who was accused of wiring money in 2007 and early 2008 from the general account to a personal account in order to cover stock market losses, according to Jackson County prosecutors
- If convicted, he could face 20 years in prison
Recent Fraud Schemes

Fictitious Entry – Line of Credit
U.S. Attorney’s Office July 23, 2012
Central District of California

• A vice president and branch manager of a Laguna Hills branch was sentenced this afternoon to 41 months in federal prison and just over $1.8 million in restitution for stealing nearly $2 million from a customer’s account
• The branch manager withdrew money from a line of credit in the name of a trust that held an account at his bank
  – To cover up the scheme, he made interest payments on the money supposedly loaned to the trust
• The branch manager “stole almost $2 million dollars from a client for a personal venture where he was trying ‘to hit it big,’” according to a sentencing memo filed by prosecutors
  – “Much like gambling, [the branch manager] used the money on a start-up company that he was intimately involved in and where he could win or lose. Like most risky gambles, he ultimately lost it all.”
Fictitious General Ledger Entry – Preventative Techniques

• Effective reconciliation of general ledger accounts:
  • All general ledger balance sheet accounts and in-house deposit accounts should be properly reconciled (the general ledger/in-house deposit account balance agreed to a subsidiary record, reconciling items adequately dated/described and followed to clearance, and the reconcilement form signed/dated by a preparer and approver) on a timely basis
  • In addition, reconciling items should clear the accounts timely and properly

• Segregation of Duties

• Effective Supervision
Phishing Scams

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)
SUBJECT: Consumer Alert
Summary: *E-mails fraudulently claiming to be from the FDIC are attempting to get recipients to click on a link, which may ask them to provide sensitive personal information. These e-mails falsely indicate that FDIC deposit insurance is suspended until the requested customer information is provided.*

The Federal Deposit Insurance Corporation (FDIC) has received numerous reports from consumers who received an e-mail that has the appearance of being sent from the FDIC. The e-mail informs the recipient that "in cooperation with the Department of Homeland Security, federal, state and local governments..." the FDIC has withdrawn deposit insurance from the recipient's account "due to account activity that violates the Patriot Act." It further states deposit insurance will remain suspended until identity and account information can be verified using a system called "IDVerify." If consumers go to the link provided in the e-mail, it is suspected they will be asked for personal or confidential information, or malicious software may be loaded onto the recipient's computer.

This e-mail is fraudulent. It was not sent by the FDIC. It is an attempt to obtain personal information from consumers. Financial institutions and consumers should NOT access the link provided within the body of the e-mail and should NOT under any circumstances provide any personal information through this media.
Phishing Scams – Preventative Techniques

• Never follow a link in an email and reveal personal data
  – Go to websites independent of the email

• Use non-internet means (ex. a phone call) to verify a source
  – In doing so, do not accept a phone number in the email (use outside source)

• Ensure that email firewalls are current and frequently tested
Recent Fraud Schemes

Cyberattacks on US Banks 10-19-2012

• The attacks bring to at least nine the number of U.S. banks targeted since Bank of America experienced a similar attack in September
  – Defense Secretary Leon Panetta last week called the attacks "unprecedented" in their velocity
• The Izz ad-Din al-Quassam Cyber Fighters, a group that has claimed responsibility for the offensive, vowed to continue through at least Thursday, 18 October
• The group says it is waging the campaign in retaliation for an American-made, anti-Islamic film
  – A trailer for the movie that appeared on YouTube set off anti-American demonstrations last month in several Middle East countries
• The latest attacks come amid reports that attackers with ties to the government of Iran have launched the attacks on banks
  – Though Panetta did not charge Iran with sponsoring the attacks, the secretary said the country has "undertaken a concerted effort to use cyberspace to its advantage."
• For its part, Iran has denied any role in the slowdowns
Hacktivists Threaten Five Banks with More Cyberattacks
December 12, 2012

• Hacktivists who claim responsibility for a series of cyberattacks on at least ten banks worldwide are vowing to reprise the electronic assaults on five of them in the coming days
• The al Qassam Cyber Fighters Group said late Monday it would target JPMorgan Chase (JPM), Bank of America (BCA), U.S. Bank (USB), PNC Financial (PNC) and SunTrust (STI) as part of a second phase of its operation
• The group added that if the "film is going to be eliminated from the Internet, the...attacks also will be stopped."
• For its part, YouTube told American Banker in November the trailer comports with the company’s content guidelines
• The attacks would constitute a repeat assault on the banks, which all saw their websites slow during a string of so-called denial of service attacks in September that U.S. officials called unprecedented in their scale and speed
• Other banks that have endured the assaults include Wells Fargo (WFC), BB&T (BBT), HSBC (HBC), Capital One (COF) and Regions Financial (RF)
Recent Fraud Schemes

Data Breach

- Heartland Payment Systems Inc. said that cyber criminals compromised its computer network, gaining access to customer information associated with the 100 million card transactions it handles each month.

- The company said it couldn't estimate how many customer records may have been improperly accessed, but said the data compromised include the information on a card's magnetic strip — card number, expiration date and some internal bank codes — that could be used to duplicate a card.

- Heartland processes transactions for more than 250,000 businesses nationwide, including restaurants and smaller retailers.

- Avivah Litan, an analyst at research company Gartner, called it the largest card-data breach ever, based on her conversations with industry executives.

Source: American Banker
Recent Fraud Schemes

Data Breach Response

• Forcht Bank said that it had been informed of the breach by its debit card processor, Heartland Payment Systems
  – The breach would allow the hackers to create duplicate debit cards

• About 8,500 of Forcht’s cards could potentially be impacted, but the bank said no fraudulent activity on the cards has been reported

• The bank said it will issue new cards and is notifying all affected customers by mail and phone calls

• A spokesman for Forcht said it had been told that other banks were likely involved, but Forcht wanted to be “out in front” in informing its customers

Source: American Banker
Recent Fraud Schemes

Data Breach Response

- Heartland Payment Systems Inc. has begun commercial testing of its end-to-end encryption system for card transactions.

- "Our fully encrypted end-to-end terminal solution is currently being-beta tested at 10 merchant locations," Robert O. Carr, Heartland's chairman and chief executive officer, said during a conference call to discuss the Princeton, N.J., transaction processor's second-quarter results. "We expect to be offering merchants our new 'E3' product with what we believe will be the highest level of data security in the market in the near term."

Source: American Banker
Data Breach – Preventative Techniques

• Compliance with all aspects of the Gramm-Leach-Bliley Act (GLBA)

• If a breach occurs, follow FFIEC Guidance—Security Breaches:
  
  • “Assess the nature and scope of an incident and identify what customer information systems and types of customer information have been accessed or misused”

  • “Notify its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information”

  • “File a timely Suspicious Activity Report (SAR), and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notifying appropriate law enforcement authorities”

  • “Notify customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it”
Poll #4

If you receive an unusual email asking you to “follow a link and give personal data”, you should?

a) Use non-internet means (ex. a phone call) to verify a source. In doing so, do not accept a phone number in the email (use outside source).

b) Do a “Reply Email” and ask if it is legitimate

c) Follow it if it is from a Federal Agency

d) All of the above
Poll #4

Answer

a) Use non-internet means (ex. a phone call) to verify a source. In doing so, do not accept a phone number in the email (use outside source).
Summary/Conclusions

- Fraud in financial institutions is significant and increasing
- Certain frauds (ex. mortgage fraud) occur during the “good times” and are found long after the fact
- Fraud perpetrated via electronic banking channels continues to change as technology changes
- All employees need to be aware of “fraud red flags”
- Implementing sound internal controls and fraud detection tools are critical in preventing financial institution fraud
Questions?

Mike Thomas
Crowe Horwath LLP
mike.thomas@crowehorwath.com
404-442-1607