Managing Emerging Technology Risk

FDIC New York Regional Office

May 16, 2012

Introductory comments

Good Afternoon and welcome to the NY Region regulatory call. The topic today is Managing Emerging Technology Risk.

Financial institutions are continuously making strategic decisions on IT investments to leverage technology in their efforts to better serve existing customers, attract new ones, and increase profitability in a very competitive environment. These decisions, together with internal policies and operations, expose the institution to increasing operational, reputation, and legal and regulatory risks in such areas as the safeguarding of customer information and fraud prevention.

IT threats continue to change and evolve quickly, presenting institutions with new security and data integrity challenges. Weaknesses in an institution's information security program can lead to financial loss, identity theft, and loss of customers. To address the specialized nature of technology related supervision, the FDIC routinely assesses financial institutions' information security programs through our on-site information technology (IT) examination program, regulatory reports and news events.

The FDIC also analyzes emerging cyber threats and bank security breaches.

The information presented today will hopefully provide you with an understanding of how the FDIC, in its role as your primary financial regulator, identifies and monitors technology related issues in the banking industry

Slide 1

Slide 2

This slide lists the payment systems that financial institutions can utilize in the US.

Today we will focus on risks revolving around the ACH system.

Slide 3

When conducting Safety & Soundness Exams – the payments review would assess areas such as Credit Risk, Liquidity Management, and Business Strategy.

Under Compliance – we review compliance with Reg. E, Disclosure Requirements, and Consumer Protection/UDAP.

AML/Risk Analysis – BSA, Money Laundering, and OFAC.

Under Technology Supervision – our staff is focused on areas such areas as Operations Risk, Vendor Management, and the Bank Service Company Act.

The increasing trend in security incidents resulting from payment systems risk as financial institutions compete in offering these services to their customers is also a focus for our IT examination staff.

Slide 4

One of the payment systems that have been frequently targeted by fraudsters is the ACH system.

Corporate Account Takeover is a type of corporate identity theft in which cyber-predators steal a business' valid online banking credentials in order to gain access to their business accounts.

There are various methods cyber predators use to gain access to the legitimate banking credentials from businesses, including mimicking an institution's website, using malware and viruses to compromise the business' system, or using social engineering to defraud employees into revealing security credentials or other sensitive data.

Systems may be compromised by:

An infected document attached to an e-mail

Employees visiting social networking sites – and clicking on infected documents, videos, or photos posted to these sites

A link within an e-mail that connects to an infected website

In each case, fraudsters exploit the infected system to obtain security credentials so they can initiate funds transfers by ACH or wire transfer to the bank accounts of associates within the U.S. or directly overseas.

Slide 5

There have been noted attacks involving perpetrators sending emails supposedly coming from the National Automated Clearing House Association – otherwise known as NACHA. NACHA is the national electronic payments association that establishes the rules and procedures governing the exchange of ACH payments. The email sent by the perpetrators reports a rejected ACH transaction and includes a link for an unauthorized ACH transaction report. If the recipient clicks on the link, malware or malicious software is downloaded to the computer.

When keylogging software is installed perpetrators can access and review the account details of the business including deposit/withdrawal patterns, ACH and wire parameters and frequency limits.

Many businesses that experienced losses failed to use ACH anti-fraud tools such as: debit block and debit filter.

Without a debit block in place, any ACH will post to an account, regardless of whether it is properly authorized. The only drawback may be that, all electronic debits will be rejected before posting to your account and returned to the originator for review.

An ACH debit filter is an electronic payment authorization service that forwards to the issuing company any transactions not authorized under specific, pre-established screening criteria for review. Such debits may be rejected depending upon the guidelines established between the company and the financial institution. The ACH Filter service gives you the flexibility to authorize single, multiple or recurring ACH debits, or to authorize an exact or maximum amount of any electronic debit transaction.

We would like to also note that although corporate accounts are targeted due to their larger balances, the ensuing discussion is also relevant to individual account takeovers.

Slide 6

Thank you, Stephanie, and good afternoon, everyone.

The material I will be presenting today is nationwide, excerpted from an internal report for FDIC use only, and is assembled quarterly by our Cyber Fraud and Financial Crimes Section from Suspicious Activity Reports (SARs), security incident reports filed by our institutions, and from internally generated information. The most recent data has been compiled for the third quarter of 2011.

Here are some highlights from that quarter's compilation of data which I will provide in more detail later:

Financial institutions, their customers, and technology service providers are detecting a higher proportion of Online Bank Account Takeovers

Because online bank accounts are harder to takeover, cyber criminals will target bank networks and employee desktops to initiate unauthorized ACH and wire transfers. Cyber criminals will also use diversionary distributed denials of service attacks (DDOS) to avoid detection by saturating or flooding a computer network with multiple commands.

Cyber criminals will also attempt online bank account takeovers in combination with email, call center, and phone banking applications.

Wire Transfer Fraud reports increased significantly during the quarter as cyber criminals continued to attempt unauthorized ACH and wire transfers via other channels.

Losses from Online bank account takeovers were well represented in wire transfer fraud reports, a large proportion of account takeovers were also perpetrated via email.

In the following 11 slides and charts, I will just point out the significant results and allow the audience to glean other pertinent and comparative data directly from the graphs.

Slide 7

Slide 8

As illustrated on the chart, computer intrusion reports fell during the quarter 16 percent to 331; during the same period, losses declined six percent. The average loss remained about the same at approximately $25,000. Total loss due to computer intrusions of all types was about $7 million during the quarter.

Slide 9

Here we present 3rd qtr 2011 data for reported computer intrusions. Note that seventy percent of all computer intrusion losses were related to online account takeovers through ID theft, Wire and ACH fraud.

In addition, during the 4th quarter of 2011, our data showed that 75% of all reported computer intrusions were online bank account takeovers.

What portals do the hackers use to gain ingress to the information needed? Compromises on FI's networks caused 27% of the sampled losses, and credit card compromises also contributed to 27% of the losses. In the 4th quarter of 2011, malware identified on customers' PCs resulted in 47% of losses for computer intrusions reported.

Slide 10

Financial institution and customer monitoring diligence have proven successful in identifying computer intrusion attempts. Computer intrusion detection rates improved from 76% in the 2Q11 to 85% during 3Q11 as depicted on the chart. From the chart, you can see that FI customers detected 38% of reported computer intrusions in the sample (blue area upper right); 17% of intrusions reported by FI employees (light maroon area); and 10% detected by card networks or their payment processors (light blue).

However, in the 4th quarter of 2011, 47% of the 306 computer intrusions reported went undetected and the average loss increased to $31,000.

Slide 11

Online bank account takeover losses totaled approximately $15 million (derived from computer intrusions, wire transfer fraud, and other SARs). Note the significant decline from the 4th quarter of 2010. Overall our data showed that online bank account takeovers fell 42% in all of 2011 compared to 2010.

Regrettably, even our most diligent preventative measures can be circumvented.

Premier hackers' toolkits can be purchased over the Internet. One such kit is SpyEye, which can be purchased for $6,000 and is surpassing the Zeus botnet as the malware of choice. The infected PC actually shows yesterday's balance to the customer so that they cannot see the unauthorized transfer initiated by the fraudster. Some red flags to the consumer would be unusual screenshots or inability to access one's online account, usually caused by a distributed denial of service attack (DDOS) described earlier.

SpyEye

- Waits for the account holder to log into his or her online banking account.
- Collects the user's balance figure and determines whether the account is ripe for theft.
- Initiates money transfers invisibly.
- Transfers funds into a mule account that is set up and controlled by the thief to receive cash transfers (almost always in a foreign country).
- Erases any evidence of the fraudulent transfer.
- Adds the stolen amount back to the official account balance, as if nothing is amiss.

Preventative guidance on corporate account takeovers is publicly available on the IC3.gov (Internet Crime Complaint Center) website, a partnership between the FBI, National White Collar Crime Center, and the Bureau of Justice Assistance. The participating agencies on one such Fraud Advisory recommend customers use a separate, locked-down PC for online banking transactions.

Slide 12

Reports of Identity Theft declined 3 percent to over 7,700 during the quarter. However, note the significant decline from the 2008 period.

Slide 13

Now we will present some data specifically pertaining to wire fraud activities. Wire transfer fraud reports jumped 21 % to over 4,000. Mortgage fraud, false statements, and commercial loan losses caused the most losses during the quarter as depicted on the following slide.

Slide 14

Fifty-six percent of wire fraud losses were mortgage fraud-related. Fifteen percent of wire transfer fraud losses related to credit card and commercial loans. Criminals are transmitting unauthorized ACH and wire transfers to more locations to avoid detection. More unauthorized transfers are going to Asia and Australia.

Data for the 4th quarter of 2011 showed that mortgage fraud represented 40% of the losses.

Slide 15

Eighty-nine percent of sampled financial institution (FI) wire fraud losses were online (34 percent), corporate (32 percent), or consumer (23 percent) account takeovers.

Slide 16

Customers suffered wire transfer losses mostly from Internet classified advertisement purchase scams (autos, trucks, and boats) and romance scams, which accounted for half of their losses. Customers also experienced losses from online banking and email account compromises.

Slide 17

Online bank account takeovers caused the most combined wire transfer loss to both financial institutions and customers according to a sample of reports - 31%, followed by corporate account takeover – 24% and customer account takeover-17%

Slide 18

Wire Transfers originated by email caused the highest proportion of total losses in the sample - 30%, followed by online classifieds, branch, and Phishing/malware attack vectors.

Slide 19

In the interests of time, instead of a graphical representation, I'll summarize what we are seeing in the area of debit card fraud. As most of you are well aware, debit card fraud reports are higher; however, losses remain about the same. Criminals are developing ways to exploit the timing differences between the point-of-sale approval, memo posting, and final transaction settlement. This is allowing overages and overdrafts that lead to losses.

Criminals are using social engineering to encourage POS terminal cashiers to "force post" transactions (without proper authorization), which also creates overdrafts and losses. Foreign debit card transactions are causing more losses due to timing differences particularly with travel-related debit transactions.

In the 4th quarter of 2011, counterfeit card crime ring reports were associated with the most losses to financial institutions. The most common counterfeit card reports were simple unauthorized charges where the origin of the breach was not reported. Two-thirds of reported counterfeit card crimes are committed by unknown suspects. California, New York, Georgia, and Texas had the most identified suspects. The data also indicated that a payment processor breach in 2009 was identified in 17% of losses during the 4Q11.

Slide 20

It is very important for each institution to implement the appropriate controls to protect itself and its customers. The following slides identify controls that should be considered in order to prevent and mitigate the risk of account takeovers of both business and consumer account credentials.

Examples include:

-Using multi-factor authentication

-Using firewalls, security suites, anti-malware and anti-spyware on all computers

-Requiring Originators and Third-Party Senders to incorporate minimum levels of security on their internal computer networks

-Separation of Duties - Initiate payments under dual control

-Create strong passwords, including lower- and upper-case letters, numbers, and special characters.

-Avoid using automatic login features and Prohibit the use of "shared" usernames and passwords for online banking systems

Slide 21

Limit administrative rights on users' workstations to help prevent inadvertent downloading of malware such as viruses, worms and spyware.

Immediately escalate any suspicious transactions to the individual or team that is responsible. This will trigger bank's internal incident response procedures for handling such security incidents.

Another control would be to clear your browser cache. To speed access to pages you have already visited, your browser often keeps a copy of the page. This data includes your browsing and download history, cache, cookies, passwords, and saved form data. The only way to be sure that any sensitive information is not inadvertently stored locally is to empty or clear your browser's cache after each online session. The instructions for clearing the cache and cookies might be different for each browser and version. However, when you open the browser, look in the Tools menu, and choose Options or Preferences. Look for an option to delete browsing history.

Regularly train your staff so they will understand your institutions internal procedures.

Educating business clients on prevention, detection and reporting measures; and encouraging daily review of accounts is also important.

Slide 22

The most recent onsite examinations conducted across the NY region have noted several findings that continue to remain prominent under the area of IT supervision. By identifying these examination findings today we hope to assist you in determining your level of compliance in the areas noted. This will also help you understand the expectations of the IT field examiners.

Slide 23

One of the areas under Section 501(b) of GLBA that we continue to see findings is in the bank's efforts to implement an adequate risk assessment. A risk assessment is a multi-step process of identifying and quantifying risks to information and infrastructure assets. Identification of sensitive, critical, and material information assets is an important first step of a risk assessment. Institutions should also consider the nature and type of information that may be processed or handled by external relationships and the ability to control that information. Management should also identify the procedures in place to ensure an effective process to adjust the program – meaning when the bank makes changes to the technology and its business function, the IS program should be updated to reflect those changes. Changes can include new system configurations, new software, software patches, mergers, and new outsourcing arrangements.

Other areas reviewed under GLBA include the reporting process for communicating the program status to the board. Reports to the board should at a minimum describe material risk issues, changes/updates to the risk assessment, service provider oversight, results of testing mitigating controls, and the impact of security breaches. IT examiners are also evaluating whether bank employees are receiving regular security awareness training.

In conjunction with the areas just mentioned, the bank's vendor management program is also assessed to determine if the third party service provider contracts include provisions related to subcontractor arrangements and adequate disposal of the bank's sensitive customer information by the service provider.

Common examination findings identified across the region related to GLBA include:

- Risk assessments that are not being updated on a regular basis to reflect changes in new systems and/or consumer services
- Management does not always identify the location of all non-public customer information
- Not testing mitigating controls or testing not properly documented
- Lack of disposal procedures
- Bank management not performing annual comprehensive board reporting
- Lack of internal vulnerability assessments or penetration testing
- Information security awareness training is not regularly conducted
- Inadequate oversight of vendor due diligence process – vendor contracts not containing necessary security provisions – vendor risk rating not properly documented- vendor risk assessments are incomplete and not properly monitored

Another area of supervisory concern is business continuity and disaster recovery (DR) plans. The primary goals of these plans are to protect personnel and customers, minimize damage to resources, and to resume operations as quickly as possible. Depending on the type and severity of the disaster, restoring operations may involve activating the recovery plan and relocating operations to temporary site.

Onsite examination revealed disaster recovery plans failing to identify critical business systems, either no annual testing or no departmental plans, Inadequate or absent pandemic plans, and insufficient or nonexistent board reporting related to disaster recovery testing results.

Common examination findings related to weak operational oversight include out of date or inaccurate information in policies, lack of IT strategic plans, and inconsistent performance of user access/entitlement reviews.

We have also noted poor IT audit coverage and untimely resolution and/or tracking of audit (or regulatory) exceptions.

As stated earlier, this is designed to help you understand how we evaluate a bank's IT area. We want to encourage bank management to monitor their IT area. We all know technology is not static. Management should adjust policies/procedures, risk assessments, and DR plans as systems/services change, and update IT strategic plans to align with the institution's overall business plan. And of course keep the BOD informed.

Slide 24

We will now discuss recent technological advances (mobile devices, social networking, and cloud services) and the risks to our financial institutions. Please direct your attention to slide 24.

The first report of an unauthorized wire transfer via mobile device (smart phone) was identified during the third qtr 2011. Sufficient wire transfer information was physically extracted from the device to originate funds transfers from a different device in a foreign location.

Previous mobile device scams were orchestrated using SMS text phishing messages to gather debit card numbers and PINs to make unauthorized withdrawals at ATMs. Other mobile banking delivery channels are via Internet browser or mobile app.

Financial institutions should be aware of the following risk areas when offering mobile banking to their customers:

1. Secure authentication and authorization of mobile customers; Financial institutions should implement controls to ensure that the person accessing banking services from a mobile device is, in fact, the bank's customer.

2. On-device data security; While financial institutions do not control the mobile device, they can design and build websites and applications such that sensitive account information will not be stored locally on the device or that such information is encrypted.

3. Mobile device malware and viruses; The marketplace for mobile-based antivirus and malware detection security software is developing and financial institutions should closely monitor these developments and consider whether to recommend that mobile banking customers run antivirus software on their mobile devices.

4. Data transmission security; It is possible to build and operate a "rogue" cell phone tower, trick mobile devices operating in the vicinity into connecting to the rogue tower, purposely downgrade the connection protocol to an older, less secure protocol, and then hijack the mobile session. Such a fraud could be used to compromise the security of mobile banking sessions, and

5. Compliance, legal, and reputation risk. Institution management and system designers should consult with their compliance officer during the development and implementation of mobile banking to minimize compliance risks. The compliance officer should:

    - Make certain any applicable disclosure requirements are fully accessible on the mobile device;

- Review the institution's existing compliance management system and make appropriate modifications to policies and procedures to address the products, services, and operating features of the mobile banking channel;
- Monitor on an on-going basis for any legal and regulatory changes that may be applicable to mobile banking; and

- Train institution staff regarding compliance implications of mobile banking.

Many of the risks involved with mobile banking exist in other technologies used by financial institutions. Therefore, the FDIC expects institutions to consider the same criteria when implementing new mobile technologies or outsourcing related technology services. These criteria include, but are not limited to, due diligence, risk assessment and control, vendor management, and ongoing monitoring and reporting.

Banks should refer to the FFIEC IT Handbooks on Outsourcing, Development & Acquisition, E-banking, and Security, and other guidance listed at the end of our presentation. Please also refer to the FDIC Supervisory Insights Journal Winter 2011 article on "Mobile Banking-Rewards and Risks".

Slide 25

The increasing use of social media sites and social networking such as Twitter, MySpace, Facebook) poses additional security risks to financial institutions - blurring between business and personal and professional lives, and emphasizing the importance of corporate governance in the workplace.

In one study on social media mobile applications, almost 75% of the apps failed to protect sensitive data, suggesting that there is more work to do to ensure mobile applications do not store sensitive information unnecessarily or unencrypted to prevent identity theft as discussed earlier.

The institution's reputation is the most prominent repercussion of victims of false or derogatory comments on social media sites.

It's important to keep in mind that the institution's site does not have to be the victim of the negative comment to be impacted (someone can post a comment anywhere with bank name)- need to review use of bank's name regularly

Also note that the same consumer compliance advertising regs apply to these sites.

Please refer to the FDIC Consumer News report in the Winter 2010 edition "Social Networking Sites Attract Online Criminals", and in the article entitled "Managing Your Business's Risks Related to Social Media" (August 2010), and in the FDIC Supervisory Insights Journal Winter 2011 article on "Mobile Banking-Rewards and Risks".

Slide 26

The use of Cloud computing services presents unique risks to the institution:

If the institution engages in cloud processing, determine that inherent risks have been comprehensively evaluated, control mechanisms have been clearly identified, and that residual risks are at acceptable levels. Regardless of the deployment model (Private, Community, Public, or Hybrid) or type of service model used (Software as a Service, Platform as a Service, Data as a Service, or Infrastructure as a Service), *you should ensure that*

- Action plans are developed and implemented in instances where residual risk requires further mitigation.

- Ensure that management updates the risk assessment/vendor management/and information security policies as necessary.

- Be sure that the types of data in the cloud have been identified (social security numbers, account numbers, IP addresses, etc.) and have established appropriate data classifications based on the financial institution's policies.

- And ensure that the controls are commensurate with the sensitivity and criticality of the data, and the effectiveness of the controls are tested and verified.

- Have adequate controls in place over the hypervisor, or virtual machine manager, if a virtual machine environment supports the cloud services.

- Ensure all network traffic is encrypted in the cloud provider's internal network and during transition from the cloud to the institution's network, and that all data stored on the service providers systems are being encrypted with unique keys that only authenticated users from this institution can access.

- Unless you are using a private cloud model, determine what controls you or your service provider established to mitigate the risks of multitenancy (multiple client organizations being served).

- If you are using the Software as a Service (SaaS) model, determine whether regular backup copies of the data are being made in a format that can be read by the financial institution. (Backup copies made by the service provider may not be readable.)

- Ensure that your business continuity plan addresses contingencies for the cloud computing service.

- Ensure you have an exit strategy and de-conversion plan or strategy for the cloud services.

- Determine whether the cloud service provider has an internal IT audit staff with adequate knowledge and experience or an adequate contractual arrangement with a qualified third-party audit firm.

The aforementioned is not all-inclusive and additional guidance can be found in Appendix A of the FFIEC Outsourcing Technology Services Handbook.

Slide 27

The following two slides present FFIEC, FDIC, and other reference material relating to today's discussion. Please note that the FFIEC Retail Payment Systems Handbook was updated to reflect changes in technology and the risks associated with remote deposit capture, merchant card processing, ACH, and other emerging payment technologies.

The new FFIEC Outsourcing Technology Services Handbook became available April 6th – the principal changes to this manual were the addition of two Appendices- Cloud Computing guidance, addressed in Appendix A, and Managed Security Service Providers guidance which appears in Appendix D.

We also want to remind bank management to be cognizant of the most recent guidance related to authentication – which was issued in January 2012. Bank management should be well-versed on the requirements to satisfy the current guidance and be able to identify the need to upgrade to a more complex solution.

To meet the current guidance, many bank vendors offer a myriad of authentication solutions to their bank clients for their purchased applications and some are at an additional charge. It is up to the bank management to determine what is appropriate to implement based on their risk assessment. TSPs are being evaluated to insure the solutions they offer are compliant with the guidance. Our primary objective at our onsite examinations is to verify management understands the requirements and its efforts undertaken to meet that goal.

Slide 28

Slide 29

We realize that our financial institutions are doing what they can to alleviate the onslaught of cyber threats and comply with regulations and guidance.

Please feel free to contact your regional or area office representatives with any questions or concerns. Our Region's contact information can be found on Slide 30.

Thank you for your participation on today's call.

We will now open the line for questions.