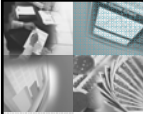





# Corporate Account Takeover

*Southwest Treasury Expo*  
25 Years. The Silver Lining

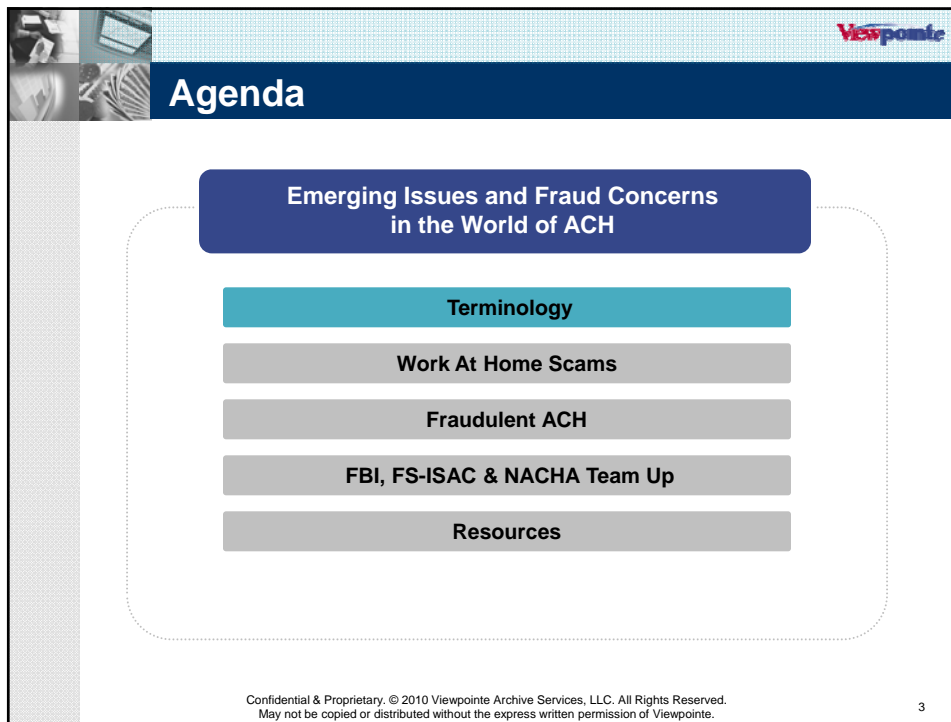



## Disclaimer

This course provides an emerging issues and fraud concerns in the world of Automated Clearing House (ACH) payment system for the ODFI and Originator. Responsibility for compliance with all legal and regulatory requirements remains at all times with individual users. This presentation and the information contained in it are not intended to be used as legal advice and Viewpointe provides this material "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein.

The information in this document and discussed in this presentation is the exclusive property of Viewpointe Clearing, Settlement & Association Services, LLC. It may not be copied, disclosed, or distributed, in whole or in part, without the express written permission of Viewpointe. © 2010 Viewpointe Clearing, Settlement & Association Services, LLC. All rights reserved.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.



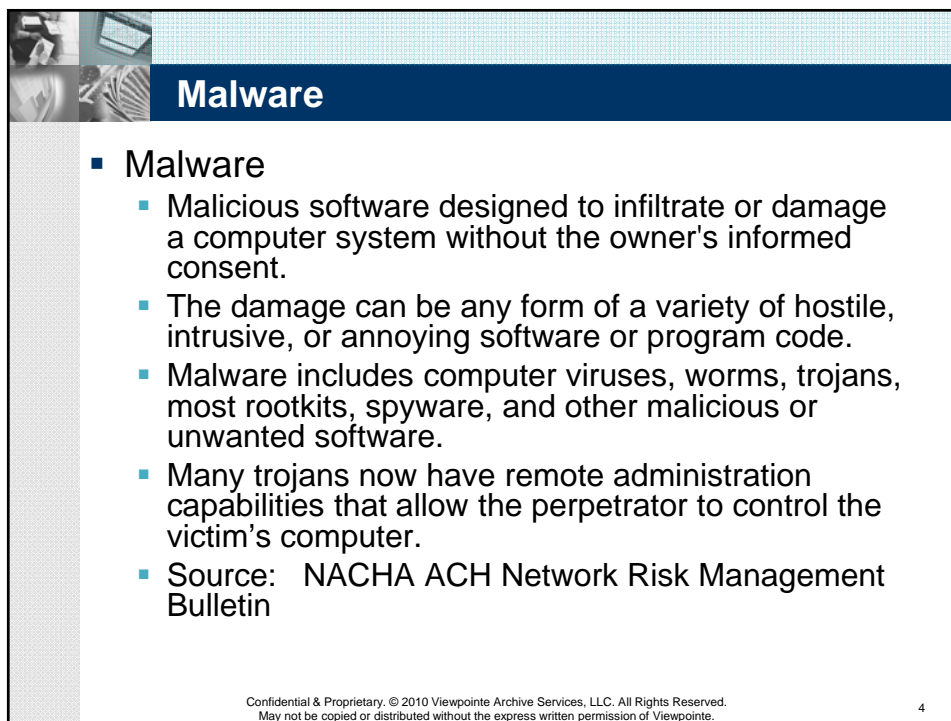
**Agenda**

**Emerging Issues and Fraud Concerns in the World of ACH**

- Terminology**
- Work At Home Scams**
- Fraudulent ACH**
- FBI, FS-ISAC & NACHA Team Up**
- Resources**

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

3

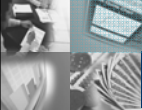


**Malware**

- **Malware**
  - Malicious software designed to infiltrate or damage a computer system without the owner's informed consent.
  - The damage can be any form of a variety of hostile, intrusive, or annoying software or program code.
  - Malware includes computer viruses, worms, trojans, most rootkits, spyware, and other malicious or unwanted software.
  - Many trojans now have remote administration capabilities that allow the perpetrator to control the victim's computer.
  - Source: NACHA ACH Network Risk Management Bulletin

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

4

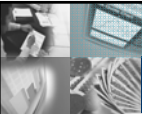


## Rootkit & Trojans

- **Rootkit**
  - Program or combination of several programs designed to hide or obscure the fact that a system has been compromised.
  - A fraudster may use a rootkit to replace system executables, which may then be used to hide processes and files that the fraudster has installed.
- **Trojans**
  - Programs that appear to have some useful purpose, but in actuality contain malicious functionality.
  - Trojan software hides its destructive portion during installation and program execution, often preventing anti-malware from recognizing it.
- **Source:** NACHA ACH Network Risk Management Bulletin

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

5

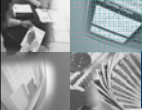


## Spyware

- **Spyware**
  - Software that is installed surreptitiously on a computer to intercept or take partial control over the user's interaction with the computer without the user's informed consent.
  - While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, or redirecting web browser activity.
- **Source:** NACHA ACH Network Risk Management Bulletin

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

6

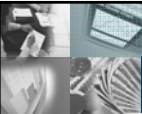


## Keystroke Logging

- Keystroke logging (often called keylogging)
  - The practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
  - There are numerous keylogging methods, ranging from hardware and software-based to electromagnetic and acoustic analysis
    - Hardware attached to computer (some look like flashdrive)
    - Software loaded to the computer
      - Many times without your knowlegde
- Why do they exist?
  - Used to track children or spouse
  - Used to track employees on work computers

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

7

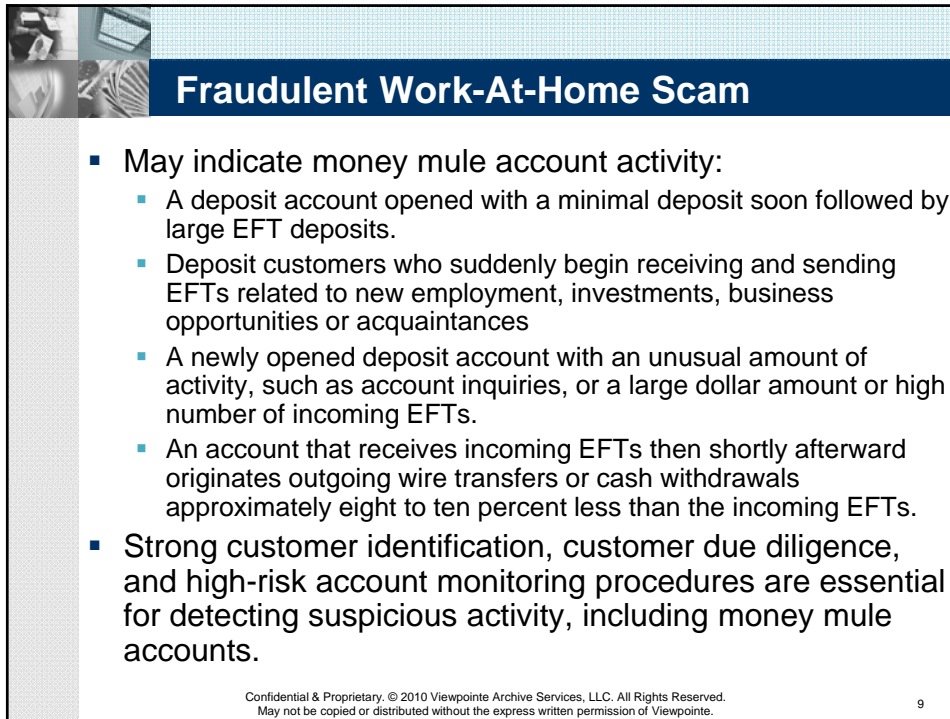


## Fraudulent Work-At-Home Scam

- The Federal Deposit Insurance Corporation (FDIC) is warning financial institutions of an increase in schemes to recruit individuals to receive and transmit unauthorized electronic funds transfers (EFTs) from deposit accounts to individuals overseas.
  - These funds transfer agents, often referred to as "money mules," are typically solicited on the Internet by criminals who have gained unauthorized access to the online deposit account of a business or consumer.
  - In a typical scenario, the criminal will originate unauthorized EFTs from a victim's account to a money mule's deposit account.
  - The money mule is then instructed to quickly withdraw the funds and wire them overseas after deducting a "commission" (commonly eight to ten percent).
- <http://www.fdic.gov/news/news/specialalert/2009/sa09147.html> for more information on fraudulent EFT schemes
- Source: FDIC Alert issued October 29, 2009

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

8

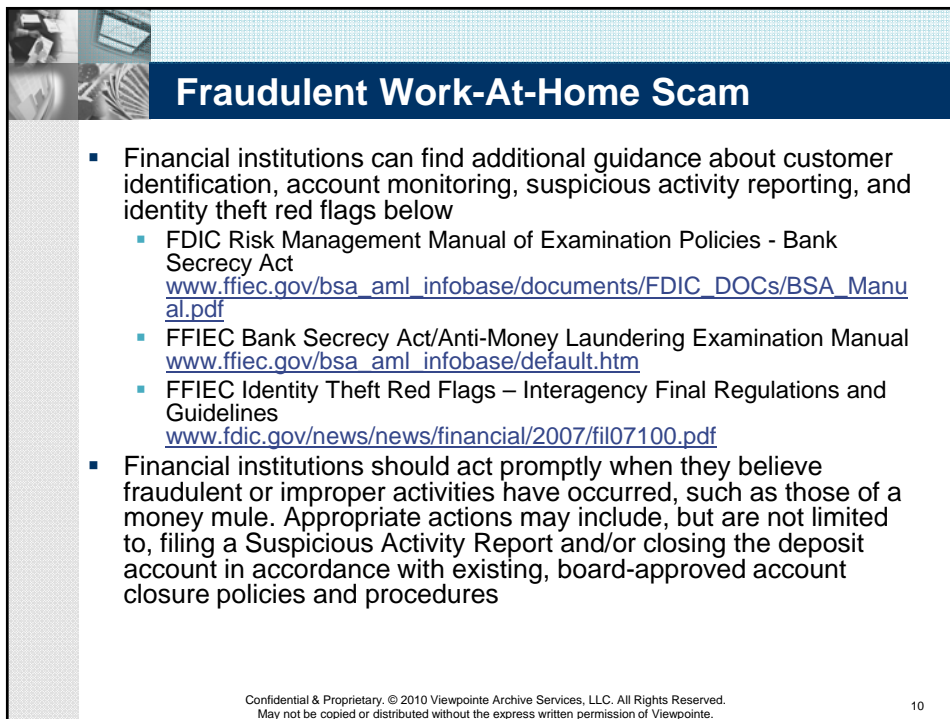


## Fraudulent Work-At-Home Scam

- May indicate money mule account activity:
  - A deposit account opened with a minimal deposit soon followed by large EFT deposits.
  - Deposit customers who suddenly begin receiving and sending EFTs related to new employment, investments, business opportunities or acquaintances
  - A newly opened deposit account with an unusual amount of activity, such as account inquiries, or a large dollar amount or high number of incoming EFTs.
  - An account that receives incoming EFTs then shortly afterward originates outgoing wire transfers or cash withdrawals approximately eight to ten percent less than the incoming EFTs.
- Strong customer identification, customer due diligence, and high-risk account monitoring procedures are essential for detecting suspicious activity, including money mule accounts.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

9

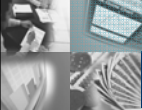


## Fraudulent Work-At-Home Scam

- Financial institutions can find additional guidance about customer identification, account monitoring, suspicious activity reporting, and identity theft red flags below
  - FDIC Risk Management Manual of Examination Policies - Bank Secrecy Act  
[www.ffiec.gov/bsa\\_aml\\_infobase/documents/FDIC\\_DOCs/BSA\\_Manual.pdf](http://www.ffiec.gov/bsa_aml_infobase/documents/FDIC_DOCs/BSA_Manual.pdf)
  - FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual  
[www.ffiec.gov/bsa\\_aml\\_infobase/default.htm](http://www.ffiec.gov/bsa_aml_infobase/default.htm)
  - FFIEC Identity Theft Red Flags – Interagency Final Regulations and Guidelines  
[www.fdic.gov/news/news/financial/2007/fil07100.pdf](http://www.fdic.gov/news/news/financial/2007/fil07100.pdf)
- Financial institutions should act promptly when they believe fraudulent or improper activities have occurred, such as those of a money mule. Appropriate actions may include, but are not limited to, filing a Suspicious Activity Report and/or closing the deposit account in accordance with existing, board-approved account closure policies and procedures

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

10

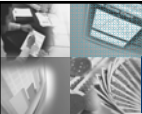


## Warning About Fraudulent ACH

- **FBI Issues Warning about Fraudulent ACH Transfers**  
 (*Payments News – Nov. 3, 2009*)  
 The FBI issued a press release earlier today highlighting concerns about an increase in ACH-based fraud targeting online banking credentials of small businesses, governments and school districts.
- [http://www.fbi.gov/pressrel/pressrel09/ach\\_110309.htm](http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm)

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

11

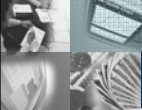


## FI Fails

- Dwelling House Savings and Loan turned over to PNC Bank
  - The takeover marks the end of Pittsburgh's only minority-owned bank and comes despite attempts to replace about \$1 million in capital that was electronically transferred from Dwelling House by thieves who remain at large. Pittsburgh police and the FBI are investigating the fraud.
- Source: TRIBUNE-REVIEW, August 15, 2009

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

12




## FBI, FS-ISAC & NACHA Team UP

- The following slides are from a joint team of the Federal Bureau of Investigation (FBI), the Financial Services Information Sharing and Analysis Center (FS-ISAC), NACHA – the Electronic Payments Association, and other Federal Government Agencies
- Account Hijacking for Corporate Customers: Recommendations for Customer Education
- Dated August 24, 2009

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

13

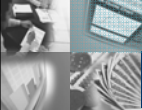


## FBI, FS-ISAC & NACHA Team UP

- FS-ISAC and NACHA recommend that all financial institutions consider implementing the following controls:
  - Strong Authentication – Financial Institutions should review the Federal Financial Institutions Examination Council's (FFIEC's) guidance, Authentication in an Internet Banking Environment (FIL-103-2005).
  - Anomalous/Fraudulent Transaction Detection - Financial institutions should implement appropriate fraud detection and mitigation best practices including transaction risk profiling.
    - [http://www.ffiec.gov/ffiecinfobase/resources/info\\_sec/2006/frb-sr-05-19.pdf](http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/frb-sr-05-19.pdf)
  - Out-of-Band Transaction Authentication – Consider using manual or transaction authentication systems in concert with fraud detection.
  - Network Defense-in-Depth - Institutions should implement a best practice, layered Defense-in-Depth to their network and system infrastructure. This Defense-in-Depth should include both technical and procedural controls.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

14




## FBI, FS-ISAC & NACHA Team UP

- Guidance from regulatory agencies has not, to date, focused on account compromise issues surrounding corporate customers. The FS-ISAC and NACHA recommend financial institutions educate corporate and small business customers on the need to operate in a secure way as well, including:
  - Account Controls:
    - Educating customers proactively about account features that may protect their accounts, such as check cashing limitations and automated payment filters.
    - Recommend reconciliation of all banking transactions on a daily basis.
    - Recommend customers initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

15




## FBI, FS-ISAC & NACHA Team UP

- Recommend customers employ best practices to secure computer systems in their business including but not limited to:
  - If possible, and in particular for customers that do high value or large numbers of online transactions, recommend commercial banking customers carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.
    - Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information.
    - Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack their computer.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

16

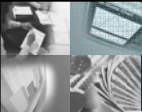


## FBI, FS-ISAC & NACHA Team UP

- Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
  - Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
  - Prohibit the use of "shared" usernames and passwords for online banking systems.
  - Use a different password for each website that is accessed.
  - Change the password a few times each year.
  - Recommend customers never share username and password information for Online Services with third-party providers.
  - Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
  - Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

17




## FBI, FS-ISAC & NACHA Team UP

- **Ensure virus protection and security software are updated regularly.**
  - Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
  - Consider installing spyware detection programs.
  - Recommend clearing the browser cache before starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.
  - Recommend customers verify use of a secure session (https not http) in the browser for all online banking.
  - Avoid using an automatic login features that save usernames and passwords for online banking.
  - Never leave a computer unattended while using any online banking or investing service.
  - Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

18

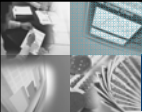


## FBI, FS-ISAC & NACHA Team UP

- Recommend customers familiarize themselves with the institution's account agreement and with the customer's liability for fraud under the agreement and the Uniform Commercial Code as adopted in the jurisdiction.
  - Stay in touch with other businesses to share information regarding suspected fraud activity.
  - Immediately escalate any suspicious transactions to the financial institution particularly, ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by the customer.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

19

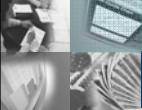


## FBI, FS-ISAC & NACHA Team UP

- The event the customer is a victim of fraud, there are a number of immediate recommendations they should take to help protect their financial interests. A few general suggestions include:-  
 Immediately cease all activity from computer systems that may be compromised. Unplug the Ethernet or cable modem connections to isolate the system from remote access.- Immediately contact their financial institution so that the following actions may be taken as a priority to contain the incident:
  - Online access to the accounts be disabled.
  - Online Banking passwords changed.
  - New account(s) opened as appropriate.
  - Request the financial institution's agent review all recent transactions and electronic authorizations on the account.
  - Additionally, ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address.- Customers can generally find customer service or fraud prevention contact telephone numbers on monthly statements. Recommending they have this information readily available will often facilitate a call.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

20

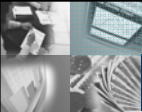


## FBI, FS-ISAC & NACHA Team UP

- Always recommend customer's suffering fraud file a police report with the local police department and provide the facts and circumstances surrounding the loss.
  - Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often facilitate dealing with insurance companies, banks, and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.
  - Maintain a written chronology of what happened, what was lost and the steps the customer took to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.
  - Realize that if the customer carries out personal online banking from the business computer system, there are also potential identify theft aspects to the compromise. Recommend the customer review the recommendation at [www.ftc.gov](http://www.ftc.gov) under identity theft
  - Dependent on law enforcement investigative and forensic considerations, recommend the customer have their network and systems reviewed by a qualified computer forensic/information security professional.

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

21




## Contact Information for Viewpointe

Kim A. Bruck, AAP  
 Manager, Association Services Member  
 Support  
 Viewpointe, LLC  
 602-443-2960  
[kim.bruck@viewpointe.com](mailto:kim.bruck@viewpointe.com)  
[www.viewpointe.com](http://www.viewpointe.com)

Confidential & Proprietary. © 2010 Viewpointe Archive Services, LLC. All Rights Reserved.  
May not be copied or distributed without the express written permission of Viewpointe.

22



**Closing Comments**

