First Choice Bank™

Best Practices*:*

Reducing the Risks of Corporate Account Takeovers

California Department of Financial Institutions – September 2012

INTRODUCTION

A state led cooperative effort, including the United States Secret Service, developed a list of recommended processes and controls for reducing the risks of Corporate Account Takeovers. These processes and controls expand upon a three-part risk management framework developed by the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), and the Financial Services-Information Sharing and Analysis Center (FS-ISAC). Fundamentally, best practices for managing this risk in terms of processes and controls centered on these three core elements:

- **Protect**
- **Detect**
- **Respond**

The following best practices have been compiled for each of the recommended processes and controls under the Protect, Detect, and Respond framework. These best practices are not an all-inclusive list and are provided as guidance to assist in implementing processes and controls needed to reduce the risk of Corporate Account Takeover thefts.

Lately, how does cybercrime work?

- Criminals target victims by scams
- Victim unknowingly installs software by clicking on a link or visiting an infected Internet site
- Fraudsters began monitoring the accounts
- Victim logs on to their Online Banking
- Fraudsters Collect Login Credentials
- Fraudsters wait for the right time and then depending on your controls – they login after hours or if you are utilizing a token they wait until you enter your code and then they hijack the session and send you a message that Online Banking is temporarily unavailable

Where does it come from?

- Malicious websites (including Social Networking sites)
- Email
- P2P Downloads (e.g. LimeWire)
- Ads from popular web sites
- Web-borne infections: According to researchers in the first quarter of 2011, 76% of web resources used to spread malicious programs were found in 5 countries worldwide ~ United States, Russian Federation, Netherlands, China, & Ukraine

It is important to remember that electronic crimes are dynamic as cyber-criminals continually change their techniques. Additional changes in risk management processes and controls will be necessary as this type of theft continues to evolve.

I. Protect

P1: Review your administrative controls over users and system configurations.

1. Implement dual control authentication for sensitive or high risk online activities including wire templates, wire approvals and ACH file approvals;
2. Periodically review employee access rights to online systems, make sure access levels are appropriate for job responsibilities;
3. Remove employee access promptly upon termination

4. Do not allow employees to maintain administrative rights on their work computers so that to prevent unauthorized software from being downloaded

P2: Educate corporate online banking users about basic online security practices

The vast majority of cyber-thefts begin with the thieves compromising the computer(s) of the business account holders. Perpetrators often monitor the customer's email messages and other activities for days or weeks prior to committing the crime. The corporate customer is most vulnerable just before a holiday when key employees are on vacation. Another risk period is on a day the business office is relocating or installing new computer equipment. Employees may be distracted and think a problem conducting online banking is due to a new network or equipment. Therefore it is important and necessary for the corporate customer's employees to follow established security practices. The institution should periodically communicate to the business account holders some or all of the following security practices that the business can implement to reduce their risks of theft. Basic practices to implement include:

1. Provide continuous communication and education to employees using online banking systems.
   a. Providing enhanced security awareness training will help ensure employees understand the security risks related to their duties;
2. Install and maintain real-time anti-virus, anti-spyware desktop firewall and malware detection and removal programs; Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans;
3. Install and Maintain Spam Filters;
4. Install routers and firewalls to prevent unauthorized access to your computer or network. Change the default passwords on all network devices;
5. Block Pop-Ups;
6. Update, on a regular basis, all computer software (operating systems and all applications) to protect against new security vulnerabilities (patch management practices);
7. Communicate to employees that passwords should be strong and should not be stored on the device used to access online banking;
8. Adhere to dual control procedures;
9. Use separate devices to originate and transmit wire/ACH instructions;
10. Transmit wire transfer and ACH instructions via a dedicated and isolated device;
11. Practice ongoing account monitoring and reconciliation, especially near the end of the day;
12. Adopt advanced security measures by working with consultants or dedicated IT staff; and
13. Utilize resources provided by trade organizations and agencies that specialize in helping small businesses.
14. Procedures to alert bank staff (including specific phone numbers and departments) when the account holder suspects a problem;
15. Subscribe to security education resources for the customer (See Appendix A) and resources that help business customers keep abreast of new and emerging issues, such as online security magazines and security vendor websites;
16. Become familiar with the applicability of laws and regulations to business owners to safeguard information. (See Appendix D).

II. Detect

Detection is closely associated with protection, as some measures to protect against electronic theft will also be an indication that a theft is being attempted. Account holders should be the most vigilant in monitoring account activity. They have the ability to detect anomalies or potential fraud prior to or early into an electronic robbery. Business account holders should be alert for some red flags related to computer and network anomalies.

D1. Detection primarily occurs through:

1. M onitoring systems;
2. Employee awareness; and
3. Recognition of symptoms of some computer breaches

D2. Warning signs or red flags visible to a business or consumer customer that their system/network may have been compromised in the possible takeover of a business account include:

a. Password no longer works
b. Inability to log into online banking system (thieves could be blocking the online access while they are making modifications to account settings);
c. Dramatic loss of computer speed;
d. Changes in the way web pages, graphics, text or icons appear;
e. Computer lock up so the user is unable to perform any functions;
f. Unexpected rebooting or restarting of computer;
g. Unexpected request for a one time password (or token) in the middle of an online session;
h. Unusual pop-up messages, especially a message in the middle of a session that says the connection to the institution's system is not working (system unavailable, down for maintenance, etc.); "try back later" or "system is undergoing maintenance";
i. New or unexpected toolbars and/or icons; and
j. Inability to shut down or restart.

III. Respond

R1. "Immediately" verify if a suspicious transaction is fraudulent.

Account holder should immediately contact bank employee. Provide primary and secondary contact information including after-hours phone numbers, and email addresses. Consider that the business's email may have also been spoofed or taken-over and may not be a secure method of communicating information.

R2. Assist bank to "immediately" attempt to reverse all suspected fraudulent transactions.

An institution's ability to recovery funds is reduced over time, measured in minutes, not hours. Thefts often include both wire transfer and ACH transfers, and could include other forms of transfers in the future. Reversals are sometimes not processed until hours or days after a transaction has already been sent and it is too late to recover the funds.

R3. Ask the bank to send a "Fraudulent File Alert" through FedLine.

Sending a "Fraudulent File Alert" through the FRB's FedLine system may help prevent receiving institutions from delivering funds to their customer (who is receiving stolen funds).

R4. "Immediately" notify the receiving institution(s) of the fraudulent transactions and ask them to hold or return the funds.

Once cyber-thieves have transferred the stolen money to another institution, the thieves will attempt to move the money out as rapidly as possible. A process/plan must be in place for notifying the institution(s) that has received the stolen money and requesting a hold on those funds. The bank may be able to react quickly to take the following steps:

1. The bank will locate phone numbers for the receiving institutions ACH departments using the FRBs FedACH directory;
2. The bank can call on the largest items first;
3. Document all calls with names, dates, and times; and
4. If the receiving institution sees that a "Fraudulent File Alert" has arrived from the FRB, they may have greater confidence that not delivering the funds to their customer will not result in liability from their customer; and
5. If the receiving institution employee is reluctant to hold the funds, remind them that this is a theft and minutes are crucial in preventing the theft from being successful. Request to speak to a supervisor.

R5. Implement a contingency plan to recover or suspend any systems suspected of being compromised.

When a system is suspected of being compromised, it is important to close off the method being used to commit the crime.

1. If it appears that online banking user credentials of an employee have been compromised, consider immediately disabling their access, and the account holder's overall access to the online banking system.
2. Depending on the size of the theft and potential losses, consider having forensic analysis performed on all suspected compromised systems as soon as possible to determine where, when and how the compromise occurred. The analysis of your system will help the institution's discovery of how the crime was committed. Coordinate with your bank on this action item.
3. Communicate frequently with your financial institution. Although the bank may be working diligently towards a full recovery of the funds; however, there is no guarantee that a full recovery will be achieved.

APPENDIX A

Resources for Business Account Holders

1. The Better Business Bureau's website on Data Security Made Simpler: http://www.bbb.org/data- security ;
2. The Small Business Administration's (SBA) website on Protecting and Securing Customer Information: http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-customer-information;
3. The Federal Trade Commission's (FTC) interactive business guide for protecting data: http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html;
4. The National Institute of Standards and Technology's (NIST) Fundamentals of Information Security for Small Businesses: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf;
5. The jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" from the U.S. Secret Service, FBI, IC3, and FS-ISAC available on the IC3 website (http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf) or the FS-ISAC website (http://www.fsisac.com/files/public/db/p265.pdf); and
6. NACHA – The Electronic Payments Association's website has numerous articles regarding Corporate Account Takeover for both financial institutions and customers: http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm.

APPENDIX B

Examples of Deceptive Ways Criminals Contact Account Holders

1. The FDIC and the NCUA do **not** directly contact institution customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC or NCUA request institution customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.
2. Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.
3. Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent statement, or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

APPENDIX C

Incident Response Plans

Since each business is unique, customers should write their own incident response plan. A general template would include:

1. The direct contact numbers of key institution employees (including after hour numbers);
2. Steps the account holder should consider to limit further unauthorized transactions, such as:
   a. Changing passwords;
   b. Disconnecting computers used for Internet banking; and
   c. Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;
3. Information the account holder will provide to assist the institution in recovering their money;
4. Contacting their insurance carrier; and
5. Working with computer forensic specialists and law enforcement to review appropriate equipment.

APPENDIX D

Information Security Laws and Standards Affecting Business Owners

Although institutions are not responsible for ensuring their account holders comply with information security laws, making business owners aware of consequences for non-compliance if the information is breached can reinforce the message that they need to maintain stronger security. Breaches of credit and debit card information from retail businesses are common. Loss of that information or sensitive personal information can create financial and reputational risks for the business.

When providing security awareness education to corporate customers, institutions may want to also alert business owners of the need to safeguard their own customers' sensitive information. California statutes related to safeguarding customer information include:

- Sections 1798.80-1798.84 of the California Civil Code, which was enacted to ensure that personal information about California residents is protected.

The Payment Card Industry Security Standards Council was launched in 2006 to manage security standards related to card processing. Any merchant that accepts credit or debit cards for payment is required to secure their data based on the standards developed by the council. The PCI Security Standards Council's website https://www.pcisecuritystandards.org/security_standards/index.php notes that noncompliance may lead to lawsuits, cancelled accounts, and monetary fines. The website provides information for small business compliance.