NACHA
The Electronic Payments Association®

Corporate Account Takeover

Prevention, Detection and Reporting for Business Customers of Financial Institutions
December 2, 2009

NACHA recommends that financial institutions educate corporate and small business customers on the need to operate in a secure way. The following are options and recommendations that financial institution can review with their customers.[1]

Account Controls

1. Reconcile all banking transactions on a daily basis.
2. Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
3. Utilize multi-factor and multi-layer authentication, for example:
    a. Something a person *knows* (user ID, PIN, password);
    b. Something a person *has* (password-generating token, USB token).
4. Utilize both routine and "red-flag" reporting on transactions.
5. Immediately report any suspicious transactions to the financial institution.
6. Stay in touch with other businesses and industry sources to share information regarding suspected fraud activity.

Computer Security Tools and Practices

1. Install a dedicated, actively managed firewall. A firewall limits the potential for unauthorized access to a network and computers.
2. Install commercial anti-virus software on all computer systems.
3. Ensure virus protection and security software are updated regularly.
4. Ensure computers are patched regularly, particularly operating system and key applications, with security patches.
5. Consider installing spyware detection programs.
6. 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. If you are not certain of the source, do not click any links.
7. Create strong passwords with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
8. Prohibit the use of "shared" usernames and passwords for online banking systems.

[1] This document is for information purposes and is not intended to provide legal advice. The guidance included is not an exhaustive list of actions, and security threats change constantly.

9. Use a different password for each website that is accessed.
10. Change the password several times each year.
11. Never share username and password information with third-party providers.
12. Limit administrative rights on users' workstations.
13. Carry out all online banking activities from a stand-alone computer system from which e-mail and Web browsing are not possible.
14. Verify use of a secure session ("https") in the browser for all online banking.
15. Avoid using an automatic login features that save usernames and passwords for online banking.
16. Never leave a computer unattended while using any online banking or investing service.
17. 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.
18. Clear your browser cache in order to eliminate copies of web pages that have been stored on your hard drive.

Recommendations for Corporate Account Takeover Victims

1. Immediately cease all activity from computer systems that may be compromised. Disconnect the Ethernet or other network connections to isolate the system from remote access.
2. Immediately contact your financial institution so that the following actions may be taken:
   - Disable online access to accounts.
   - Change online banking passwords.
   - Open new account(s) as appropriate.
   - Request the financial institution's agent review all recent transactions and electronic authorizations on the account.
   - 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.
3. Maintain a written chronology of what happened, what was lost and the steps taken 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.
4. File a police report 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.

Sources: NACHA (www.nacha.org) and the Financial Services – Information Sharing and Analysis Center (www.fs-isac.com)