

NACHA's Risk Management Services finds it necessary from time to time to inform your organization of events regarding ACH risk that is of time-sensitive importance.

Corporate Account Takeovers

August 12, 2009

Fraudsters Look for Online Credentials to Raid Small-Business Accounts

Financial institutions' business customers are being attacked by malicious software in which perpetrators are attempting to obtain their valid online banking credentials. The targets appear primarily to be small financial institutions and small-business customers that are vulnerable because they do not have or do not use the most current authentication protocols, transaction controls and "red flag" reporting. Once a business' credentials are stolen, the perpetrator has online access to the business' account and any funds transfer capabilities associated with the credentials.

Stealing Credentials

There are several methods being employed to steal credentials. One is to mimic the look and feel of legitimate financial institutions' websites. Users provide their credentials to these sites, without knowing that it is the perpetrator behind the website.

A second is malware that infects computer workstations and laptops via infected e-mails with links or document attachments. In addition, malware can be downloaded to users' workstations and laptops by visiting legitimate websites - especially social networking sites - and clicking on the documents, videos or photos posted there. The malware installs keylogging software on the computer, which allows the perpetrator to capture the user's ID and password as they are entered at the financial institution's website.

Other viruses are more robust. They alert the perpetrator when the legitimate user has logged onto a financial institution's web site, then fools the user into thinking the system is down, or not responding, when the perpetrator is actually sending transactions in the user's name.

Corporate Account Takeover

In a worst-case scenario where robust authentication is not used, once the user's credentials are stolen, the perpetrator can take over the business' account. To the financial institution, the credentials look just like the legitimate user. The perpetrator has access to and can review the account details of the business, including account activity and patterns, and ACH and wire transfer origination parameters (such file size and frequency limits, and Standard Entry Class (SEC) Codes).

With an understanding of the permissions and the limits associated with the account and the credentials, the perpetrator transfers funds out of the account using wire transfers or an ACH file. With ACH, the file would likely contain PPD credits routed to accounts at one or more RDFIs. These accounts may be newly opened by accomplices or unwitting "mules" for the express purpose of receiving and laundering these funds. The accomplices or mules withdraw the entire balances shortly after receiving the money, then send the funds overseas via wire transfer or other popular money transfer services. (cont'd on Page 2)

(cont'd from Page 1)

Perpetrators also send out ACH files containing debits in order to collect additional funds into the account that can subsequently be transferred out. The debits would likely be CCD debits to other small business accounts for which the perpetrator has also stolen the credentials or banking information. Given the 2-day return timeframe for CCD debits and the relative lack of account monitoring and controls at many small businesses, these debit transactions often go unnoticed until after the return timeframe has expired.

What can business customers do to protect themselves?

Corporate customers can take many steps to protect themselves against account takeover:

- One of the most effective, yet basic, controls is for corporate customers to always initiate ACH and wire transfer payments under dual control. For example, one individual initiates the creation of the payment file, and another approves the file for release.
- Using multiple factors to prove identity is very effective in preventing a successful attack. Multiple factors are more challenging to compromise. For example, the use of 1) something the person *knows* (user ID, PIN, password), and 2) something the person *has* (password-generating token, USB token) can substantially reduce the vulnerability to an attack. Tokens that generate single-use codes are among the best practices.
- Restrict functions for computer workstations and laptops that are used for online banking and payments. This will help to prevent the inadvertent downloading of malware or other viruses by users.
- Ensure that the corporate customer's operating system and its components are up-to-date with current software patches. For example, the use of the most current firewalls, malicious code filtering, virus protection and spyware removal software will aid in the control of network intrusion tactics.
- Corporate clients should be reconciling their bank accounts daily. Many corporate clients, particularly small business clients, may not typically reconcile their bank account on a daily basis, and therefore may not recognize fraudulent activity until it is too late to take action. "Red flag" reporting (i.e., alerts about unusual activity) may also help.

What should an ODFI do if a customer has been victimized?

- Contact appropriate law enforcement immediately.
- File a Suspicious Activity Report (SAR).
- Contact the RDFI(s) to determine if the funds have been withdrawn.
- Conduct a forensic analysis and consider suspending the Originator's funds transfer capabilities until the results are known.

Additional Guidance for Financial Institutions

The Federal Financial Institutions Examination Council's (FFIEC's) guidance, *Authentication in an Internet Banking Environment* (FIL-103-2005), addresses why financial institutions should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing Internet-based financial services. The FFIEC considers "single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties." Go to www.ffiec.gov for more information.

NACHA Risk Management Alert

is a publication of
NACHA—The Electronic
Payments Association
13450 Sunrise Valley Drive
Suite 100
Herndon, VA 20171
Phone: 703-561-1100
Fax: 703-787-0996

Editor
Jeanette A. Fox, AAP

© 2009 National Automated
Clearing House Association
All rights reserved.