

G G U I D E

YOUR MONTHLY GUIDE TO THE WORLD OF ACH

A Build Your Defense Strategy Against Corporate Account Hijackers

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. ACH Fraud scams total over \$100 million says the FBI.

C A **Defense-in-Depth strategy** that includes technical, organizational, and operational controls is strongly recommended by FS-ISAC and NACHA.

Educate your business customers on how protect themselves?

- ◆ 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.
- ◆ Require a transmittal verification. By requiring a simple fax transmittal sheet signed by an authorized signer on the account that shows file totals can alone prevent the fraud scheme. Some customers claim to be too busy for a fax transmittal but any type of shared secret incapable of being reproduced by a hijacker that proves the right person is sending the file will work.
- ◆ 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 if your business customer does not want to be bothered with controls?

Use Scare Tactics in True Stories

- ◆ http://voices.washingtonpost.com/securityfix/2009/07/clampi_trojan_the_rise_of_matr.html
- ◆ http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm
- ◆ http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html?wprss=securityfix
- ◆ http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html
- ◆ http://www.americanbanker.com/btn_issues/22_8/on-the-backs-of-mules-an-ach-fraud-scheme-1000631-1.html
- ◆ <http://www.hoax-slayer.com/fake-critical-update.shtml>
- ◆ http://www.bankinfosecurity.com/articles.php?art_id=1490

GACHA Guide # 67

December 2009