ACH Operations Bulletin

Corporate Account Takeovers Can Lead to Fraudulent Transactions

December 2, 2009
For Distribution to Participating Depository Financial Institutions

EXECUTIVE SUMMARY[1]

This ACH Operations Bulletin provides information to Participating Depository Financial Institutions about "corporate account takeover" – a specific type of cyber-crime that is targeting small- and medium-sized business customers of financial institutions.

This Operations Bulletin also provides guidance for financial institutions on steps that they and their business customers each can take to reduce their respective vulnerabilities to corporate account takeover.

WHAT IS CORPORATE ACCOUNT TAKEOVER?

"Corporate account takeover" is when cyber-thieves gain control of a business' bank account by stealing the business' valid online banking credentials. Although there are several methods being employed to steal credentials, the most prevalent involves malware that infects a business' computer workstations and laptops.

A business can become infected with malware via infected documents attached to an e-mail or a link contained within an e-mail that connects to an infected web site. 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. This malware can also spread across a business' internal network.

In a recent attack, cyber-thieves sent millions of e-mails purporting to come from NACHA. Mimicking a reputable, national organization is a common tactic used by cyber-thieves to gain credibility and lure unsuspecting individuals into taking some action. The e-mail "reported" a rejected ACH transaction, and included a link for an "Unauthorized ACH Transaction Report." A recipient who clicked on the link would be taken to a fake web site that mimicked the real NACHA web site, which prompted the recipient to click on a fake transaction report. If the recipient clicked the link, the malware was downloaded to the recipient's computer.

---

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

The malware installs keylogging software on the computer, which allows the perpetrator to capture a user's credentials as they are entered at the financial institution's web site. Sophisticated versions of this malware can even capture token-generated passwords, alter the display of the financial institution's web site to the user, and/or display a fake web page indicating that the financial institution's web site is down. In this last case, the perpetrator can access the business' account online without the possibility that the real user will log in to the web site.

Once installed, the malware provides the information that enables the cyber-thieves to impersonate the business in online banking sessions. 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 as file size and frequency limits, and Standard Entry Class (SEC) Codes).

The cyber-thieves use the sessions to initiate funds transfers, by ACH or wire transfer, to the bank accounts of associates within the U.S. These accounts may be newly opened by accomplices or unwitting "money mules" for the express purpose of receiving and laundering these funds. The accomplices or mules withdraw the entire balances shortly after receiving the money, and then send the funds overseas via over-the-counter wire transfer or other common money transfer services.

WHY ARE SMALLER BUSINESSES AND ORGANIZATIONS TARGETED?

The cyber-thieves appear to be targeting small- to medium-sized businesses, as well as smaller government agencies and non-profits, for several reasons:

1. Many small businesses and organizations have the capability to initiate funds transfers - ACH credits and wire transfers - via online banking (individual consumers generally do not have this capability except for payees set up in online bill payment systems);
   - This funds transfer capability is often related to a small business' origination of payroll payments;
   - In corporate account takeover, the cyber-thieves may add fictitious names to a payroll file (directed to the accounts of money mules), and/or initiate payroll payments off-cycle to avoid daily origination limits;
2. Small businesses often do not have the same level of resources as larger companies to defend their information technology systems;
3. Many small businesses do not utilize additional banking services, such as password-generating tokens, and do not monitor and reconcile their accounts on a frequent or daily basis;
4. Small businesses bank with a wide variety of financial institutions with varying degrees of IT resources and sophistication. Some financial institutions may not offer or require services that would defend against corporate account takeover.

WHAT CAN A FINANCIAL INSTITUTION DO?

Financial institutions and business customers have distinct responsibilities to help address the security of online access to businesses' accounts. Each can take steps to protect corporate accounts from being taken over.

The top things financial institutions can do are:

1. Deploy multi-factor and multi-channel authentication for business accounts that are permitted to initiate funds transfers. For example:
    - Something the person *knows* (user ID, PIN, password);
    - Something the person *has* (password-generating token, USB token);
2. Require their business customers to initiate payments under dual control, with distinct responsibility for transaction origination and authorization;
3. Enable "out-of-band" confirmation of payment initiation, or for certain defined types of payments;
4. Provide out-of-band alerts for unusual activity ("red flag" reports);
5. Establish and monitor exposure limits that are related to customers' activities;

Financial institutions should educate their business customers on prevention, detection and reporting measures. The top things a business can do are:

1. Initiate ACH and wire transfer payments under dual control. For example:
    - One person authorizes the creation of the payment file;
    - A second person authorizes the release of the file;
2. Ensure that all anti-virus and security software and mechanisms for all computer workstations and laptops that are used for online banking and payments are robust and up-to-date;
3. Restrict functions for computer workstations and laptops that are used for online banking and payments;
    - For example, a workstation used for online banking should not be used for general Web browsing and social networking;
    - A better solution is to conduct online banking and payments activity from a dedicated computer that is not used for other online activity, and/or is not connected to an internal network;
4. Monitor and reconcile accounts daily. Many small business clients do not reconcile their bank accounts on a daily basis, and therefore may not recognize fraudulent activity until it is too late to take action.
5. Utilize routine and "red-flag" reporting (i.e., alerts about unusual activity) for transaction activity.

ACH OPERATOR SERVICES

Financial institutions should consider fraud detection and risk management services offered by their ACH Operators. For example, a threshold or a cap on ACH credit origination could alert a financial institution, particularly a small institution with low average daily ACH credit origination, to irregular origination activity.

WHAT TO DO IF YOUR CUSTOMER IS VICTIMIZED

A financial institution whose customer has been victimized can:

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

HOW TO SPOT A MONEY MULE

The corporate account takeover scheme relies on "money mules" for the final transfer of funds out of the U.S. Money mules are typically individuals unrelated to the cyber-thieves. They are recruited either through online advertisements for work-at-home and mystery shopper schemes, or through online job sites where they have posted resumes.

Once recruited, a money mule is instructed to open a bank account. Shortly thereafter, large deposits are made into the account by ACH credit or wire transfer. The money mule withdraws the funds (less a commission or fee), and then uses an over-the-counter wire transfer service to remit the funds out of the country to his or her "employer."

To spot a money mule, a financial institution can look for a pattern of activity that is consistent with the corporate account takeover scheme:

- A new account opened by an individual consumer with a small deposit, followed shortly by one or more large deposits by ACH credit or wire transfer;
- An existing account with a sudden increase in the number and dollar amount of deposits by ACH credit or wire transfer;
- A new or existing account that withdraws a large amount of cash shortly after a large deposit by ACH credit or wire transfer (often 5-10 percent less than the deposit because the mule has withheld a commission).

In many of these cases, the dollar amounts of the deposits and withdrawals are often around $9,000, apparently due to a belief on the part of the cyber-thieves that transactions of $10,000 or more receive more scrutiny by financial institutions.

According to the FDIC, "money mule activity is essentially electronic money laundering addressed by the Bank Secrecy Act and Anti-Money Laundering Regulations. Strong customer identification, customer due diligence, and high-risk account monitoring procedures are essential for detecting suspicious activity, including money mule accounts."

ADDITIONAL INFORMATION AND RESOURCES

Banking regulatory agencies consider funds transfers initiated via Internet banking to be inherently "high-risk." The agencies consider "single-factor authentication, as the only control mechanism, to be inadequate" for securing such high-risk transactions.

Regulators and law enforcement agencies that have issued relevant guidance include:

FFIEC
Authentication in an Internet Banking Environment – October 12, 2005
http://www.ffiec.gov/pdf/authentication_guidance.pdf

E-Banking/IT Examination Handbook – August 2003
http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/e_banking.pdf

FDIC
Fraudulent Work-at-Home Funds Transfer Agent Schemes – October 29, 2009
http://www.fdic.gov/news/news/SpecialAlert/2009/sa09185.html

Fraudulent Electronic Funds Transfers (EFTs) – August 26, 2009
http://www.fdic.gov/news/news/SpecialAlert/2009/sa09147.html

FBI
Fraudulent Automated Clearing House (ACH) Transfers Connected to Malware and Work-at-Home Scams – November 3, 2009
http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm

Local FBI Offices
http://www.fbi.gov/contact/fo/fo.htm

FTC
Red Flags Rule
http://ftc.gov/redflagsrule

Internet Crime Complaint Center (IC3)
http://www.ic3.gov

Financial Services – Information Sharing and Analysis Center
http://www.fsisac.com/