Commercial Insights

American Bankers Association.

Commercial Spotlight

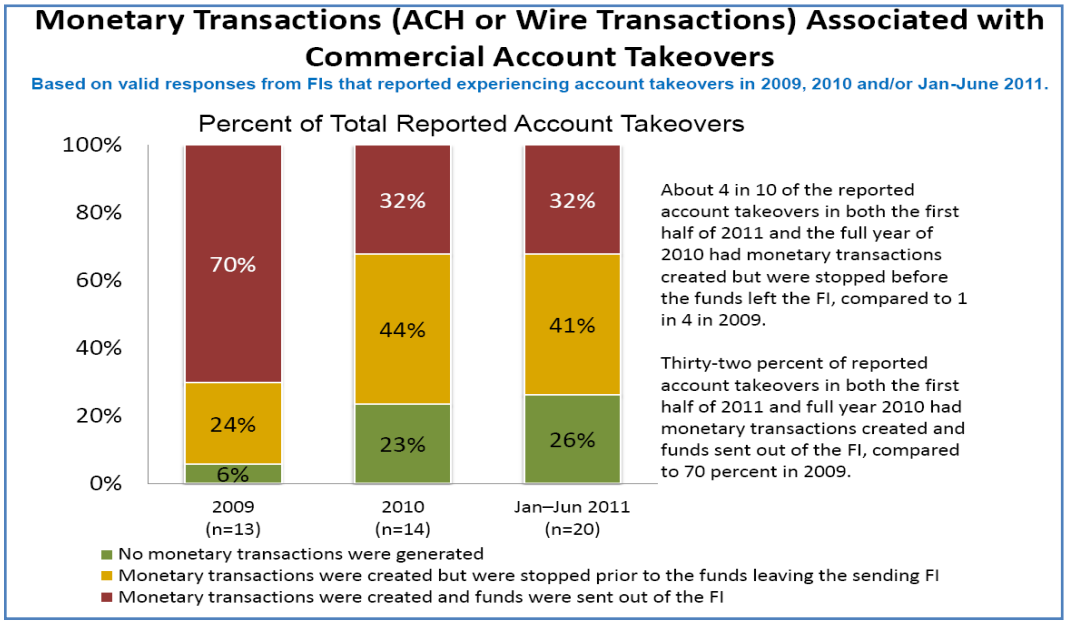
Partnering with Corporate Customers to Prevent, Detect and Respond to Corporate Account Takeover Fraud
Doug Johnson, Vice President, Risk Management Policy

As reported in *Commercial Insights* in April 2010, while millions of safe and secure electronic transactions are processed in the U.S. daily, cyber criminals are becoming increasingly adept at victimizing your business customers. One such fraud, Corporate Account Takeover (ATO), takes advantage of technological vulnerabilities and the public's limited knowledge of ever-evolving security threats associated with the Internet to attack business accounts.

The Corporate Account Takeover Threat

First identified in 2005, Corporate Account Takeover is a type of corporate identity theft in which cyber thieves steal business' valid online banking credentials or hijack browser sessions to access a customer's account. Once the cyber thief gains access to an account, they can conduct unauthorized transactions, change contact information and gather information on the account's history to commit other crimes.

Banks were initially targeted for this fraud; however, as bank security strengthened in recognition of the threat, cyber thieves set their sights on a new target: the corporate customer, targeting employees and businesses of all sizes through phishing and other social engineering attacks with the goal of enticing them to download and spread malware that will allow unauthorized access to financial accounts and other sensitive information.



Copyright 2012 – American Bankers Association, All Rights Reserved

Over time, financial institutions have proven more adept at preventing, detecting and responding to ATOs. For instance, according to a survey conducted by the FS-ISAC, while the number of attempted ATOs has been increasing in recent years, the percentage of cases where monetary transactions were created and funds were sent out of the financial institution dropped to 32 percent in 2010 and 2011 from a high of 70 percent in 2009. Nonetheless, according to the recent VeraCode *Fraud Survey of Small Business Preparedness*, 72 percent of data breach cases in 2011 affected businesses with 100 employees or less. It is thus vitally important that businesses understand and prepare for this risk.

ABA continues to be committed to addressing this issue through its participation in various collaborative working groups involving individual institutions, other industry associations, regulators and law enforcement. As a participant within the Financial Services Information Sharing Center's (FS-ISAC) Account Takeover Task Force, ABA assisted in the development of a number of resources designed to educate banks and their corporate clients on how to deter, detect and respond to this fraud.

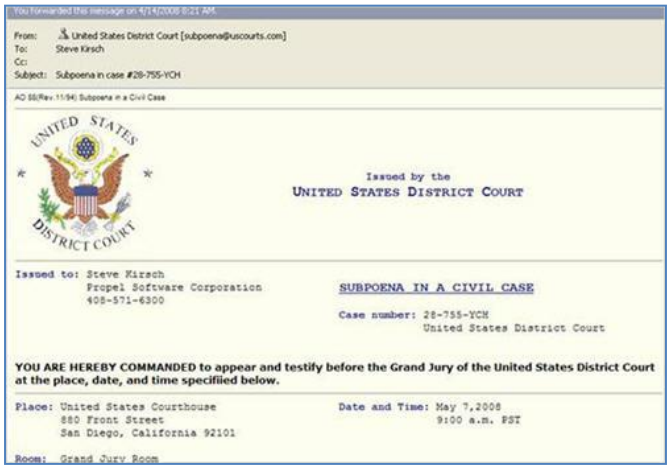
How Corporate Employees are at Risk

Any Employee is Vulnerable to Being Targeted during an ATO Attack

The most common way employees download and spread malware is by opening attachments or links in e-mails that are infected or that connect to an infected website. Cyber criminals will often "phish" for victims using mass e-mails, pop-up messages that appear on their computers and/or the use of social networking and Internet career sites. Employees typically targeted often include (but are not limited to) senior executives, accounting or human resources personnel and even business partners. Often, criminals may research their victims using social and business networking sites to gather information and better target their message to the recipient.

Cyber criminals use various methods to trick employees into opening an infected attachment or clicking on a link to an infected website, including:

- ✓ Disguising the e-mail to look as though it's from a legitimate business. Scare tactics are often used to incent employees to open the e-mail and/or provide account information. For example, cyber criminals have sent e-mails claiming to be from:
  - UPS (e.g., "There has been a problem with your shipment.")
  - Financial institutions (e.g., "There is a problem with your banking account.")
  - Better Business Bureaus (e.g., "A complaint has been filed against you.")
  - The Legal Court systems (e.g., "You have been served a subpoena.")


You forwarded this message on 4/14/2008 9:21 AM

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev. 11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

Phishing e-mails Can Look Like They Come from a Legitimate Source

Copyright 2012 – American Bankers Association, All Rights Reserved

Corporate Employee Education is Essential

Education of corporate employees has proven to be effective in reducing the threat of account takeover, yet many smaller businesses have no formal Internet security policy and many provide no Internet safety training to employees. ABA has drafted *The Small Business Guide to Corporate Account Takeover* (available online), to assist member banks with this effort.

Corporate employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices and responses to a suspected takeover are essential to protecting company and customers.

The best way to protect against account takeover is to work with your corporate customers to ensure they understand the security measures needed within the business and establish safeguards on the accounts that can help the bank identify and prevent unauthorized access to funds.

A shared responsibility between the bank and the business is the most effective way to prevent corporate account takeover.

Consider providing your corporate customers with the following tips:

- ✓ **Protect your online environment.** It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected Internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically.

- ✓ **Partner with your bank to prevent unauthorized transactions.** Talk to your banker about programs that safeguard you from unauthorized transactions. Positive Pay and other services offer call-backs, device authentication, multi-person approval processes and batch limits to help protect you from fraud.

- ✓ **Pay attention to suspicious activity and react quickly.** Look out for unexplained account or network activity, pop ups and suspicious emails. If detected, immediately contact your financial institution, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.

- ✓ **Understand your responsibilities and liabilities.** The account agreement with your bank will detail what commercially reasonable security measures are required for your business. It is critical that you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover. Talk to your banker if you have any questions about your responsibilities.

Ensuring Corporate Customers Understand Their Liability

As the last bullet in the last section implies, many corporate customers may believe that their commercial accounts are protected against fraud losses in the same manner as retail accounts when they are not. It is important that the bank ensure such customers understand their potential liability for losses incurred in commercial accounts as well as the security measures they should instill to prevent such losses.

Copyright 2012 – American Bankers Association, All Rights Reserved

Educating corporate customers regarding differences between the protections offered on retail versus commercial accounts is also now a regulatory requirement. In June 2011, the FFIEC Agencies issued a Supplement to existing customer authentication guidance, noting that a financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- ✓ An explanation of protections provided and not provided to account holders relative to electronic funds transfers under Regulation E and a related explanation of the applicability of Regulation E to the types of accounts with Internet access;
- ✓ An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials;
- ✓ A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;
- ✓ A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk or, alternatively, a listing of available resources where such information can be found; and,
- ✓ A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events.

Tying it All Together

Ensuring that corporate customers understand their responsibility for securing their accounts and their potential liability if they do not is now a vital part of the banking relationship. Accomplishing this task in a way that also ensures that the customer knows the bank is an active security partner is essential. Providing corporate customers the tools to do their part goes a long way to building this relationship.

Copyright 2012 – American Bankers Association, All Rights Reserved