CORPORATE ACCOUNT TAKEOVER (CATO)

What is Corporate Account Takeover?

Corporate Account Takeover occurs when a criminal obtains electronic access to your bank account and conducts unauthorized transactions. The criminal obtains electronic access by stealing the confidential security credentials of your employees who are authorized to conduct electronic transactions (wire transfers, Automated Clearing House-ACH, and others) on your corporate bank account. Losses from this form of cyber-crime range from the tens of thousands to the millions with the majority of these thefts not fully recovered. Corporate Account Takeovers have affected both large and small banks.

What are methods of Corporate Account Takeover?

Business Email Compromise is one of the most common methods being employed to steal confidential security credentials. This is when an unknown source gathers enough information from a business to successfully convince an employee to send funds to them or is able to do so themselves.

- Ex: Wire Transfer – urgent request, last minute update to transaction details
- Ex: Email from an employee asking to change their banking information for payroll
- Ex: Emails or calls asking to verify a small piece of information
  Often times done over a series of calls or emails to get all the details they need prior to requesting the change (Social Engineering)
- Information collected using social networking, "out of office notices, social media posts, job titles or signatures on website
- Impersonation or take over of a business email account
- Using the compromised email to achieve the goal such as requesting funds be sent to a new account or gift cards purchased (often sent as a request from a senior partner)

Phishing mimics the look and feel of a legitimate financial institution's website, e-mail, or other communication. Users provide their credentials without knowing that a perpetrator is stealing their security credentials through a fictitious representation which appears to be their financial institution.

Another common method is **Malware** that infects computer workstations and laptops via infected e-mails with links or document attachments. In addition, malware can be downloaded to a user's workstation or laptop from legitimate websites, especially social networking sites. Clicking on the documents, videos, or photos posted there can activate the download of the malware. The malware installs key-logging 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 sophisticated. They alert the perpetrator when the legitimate user has logged onto a financial institution's website, then trick the user into thinking the system is down or not responding. During this perceived downtime, the perpetrator is actually sending transactions in the user's name.

What does Corporate Account Takeover look like?

If robust authentication is not used and a user's credentials are stolen, the perpetrator can take over the account of the business. To the financial institution, the credentials appear to be the legitimate user. The perpetrator has access to, and can review the account details of, the business. These details include account activity and patterns, and ACH and wire transfer origination parameters such as file size and frequency limits and Standard Entry Class (SEC) codes.

With an understanding of the permissions and the limits associated with the account, the perpetrator can transfer funds out of the account using wire transfers or ACH files. With ACH, the file would likely contain PPD (Prearranged Payments & Deposits) credits routed to accounts at one or more receiving depository financial institutions (RDFI's). 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 and send the funds overseas via wire transfer or other popular money transfer services.

Perpetrators also send 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 (Cash Concentration & Disbursement) 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 businesses do to protect themselves?

- Education is Key – Train your employees
- Secure your computer and networks
- Limit Administrative Rights - Do not allow employees to install any software without receiving prior approval.
- Install and Maintain Spam Filters
- Surf the Internet carefully
- Install & maintain real-time Anti-Virus & Anti-Spyware Desktop Firewall & Malware Detection & Removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
- Install routers and firewalls to prevent unauthorized access to your computer or network. Change the default passwords on all network devices.
- Install security updates (patches) to operating systems and all applications as they become available.
- Block Pop-Ups
- Use strong password policies
- Do not open attachments from e-mail - Be on the alert for suspicious e-mail
- Do not use public Internet access points
- Monitor and Reconcile Bank Accounts Daily - especially near the end of the day
- Note any changes in the performance of your computer - dramatic loss of speed, computer lock-ups, unexpected rebooting, unusual pop-ups, etc.
- Make sure that your employees know how and to whom to report suspicious activity – both at your Company and your Bank
- Use multi-layer security

Contact us if you:

- **Suspect a Fraudulent Transaction**
- **Are trying to process an Online Wire Transfer or ACH Batch and you receive a Maintenance Page**
- **Receive an e-mail claiming to be from the Bank and it is requesting personal/company information**

The Bank will NEVER ask for sensitive information, such as Account Numbers, Access IDs, or Passwords via e-mail.

Incident Response Plans

Since each business is unique, customers should write their own Incident Response Plan. A general template would include:

1. The direct contact numbers of key bank employees (including after-hours numbers);
2. Steps the accountholder should consider to limit further unauthorized transactions, such as:
   a. Changing passwords;
   b. Disconnecting computers used for Internet Banking;
   c. Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;
   d. Noting information the accountholder will provide to assist the bank in recovering the accountholder's money;
   e. Contacting their insurance carrier; and
   f. Working with computer forensic specialists and law enforcement to review appropriate equipment.

Resources for Business Accountholders

NACHA – The Electronic Payments Association's website has numerous articles regarding Corporate Account Takeover for both financial institutions and banking customers: https://www.nacha.org/Corporate_Account_Takeover_Resource_Center

The Federal Trade Commission's (FTC) Interactive Business Guide for Protecting Data: http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html

The jointly-issued 'Fraud Advisory for Businesses: Corporate Account Takeover' from the U.S. Secret Service, FBI, IC3, and FS-ISAC available on the IC3 website: http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf