Dedham Savings

Business Incident Response Plan Checklist for Account Takeover

Since each business is unique, customers should write their own incident response plan. A general template would include the following:

1. Notify Your financial Institution

- ☐ Review your recent deposit account activity for authenticity.
- ☐ Request a hold be placed on your accounts to stop all activity
- ☐ Make sure all online banking functions are disabled or suspended.
- ☐ Close effected deposit account(s) and open replacement account(s). (if necessary)
- ☐ Consider changing your User ID and passwords on other systems.

2. Gather Details on the fraudulent transactions and attempt to stop transfers of funds (w/ financial institutions)

- ☐ Date(s) of incident(s):_____
- ☐ Type of Transaction involved:_____
- ☐ Request assistance from your Financial Institution to stop pending transfers as necessary.
- ☐ Dollar Amount, ABA (bank routing number), and account numbers involved:

  _____

3. Gather and document information on the incident

- ☐ How do you know about the issue? Who reported it?_____

  _____
- ☐ What is the User ID used in the incident?_____
- ☐ Was it shared?_____
- ☐ Did the user notice anything unusual during the log in process? _____

  _____
- ☐ Have you confirmed that this incident is in fact fraudulent? _____

4. Notify parties at your company

- **Management:** Oversee and coordinate process
- **IT Department**: (may be outsourced) Identify and mitigate further attacks
- **Bookkeeping/ACH Officer**: Work with bank on recovery
- **Corporate Security**: Contact law enforcement
- **Public Relations**: Work on press release if needed
- **Legal Counsel**: Consider and coordinate legal issues

5. Attempt to recover lost funds and plan for recourse

- ☐ Ask for assistance of your financial institution to reach out to the other financial institutions involved in an attempt to recover any unauthorized fund transfers.
- ☐ Determine a plan to handle legitimate online banking account functions needed during the investigation period with your financial institution. What is your plan?
- ☐ Contact your insurance company and determine what coverage you have on any loss.
- ☐ Alert employees of confirmed or suspected corporate account takeover
- ☐ Have your public relations prepare a press release (if applicable)
- ☐ Contact local law enforcement and obtain a copy of the police report.
- ☐ File a complaint with the Internet Crime Complaint Center at: www.ic3.gov

6. Identify vulnerability and begin a plan to remedy

- ☐ Does the compromised user access the online banking account via more than one computer station or by remote access?
- ☐ Is the compromised computer connected to the network?
- ☐ Has the computer(s) been checked for malware and viruses by up-to-date anti-virus software? Who conducted the scan?
- ☐ When was the last time the user legitimately logged into the online banking account? (may help to determine date of infection)
- ☐ How did the computer become infected with malware? (Opened infected email attachment, user clicked on infected website link within email, user clicked on infected document, picture, or video in legitimate website.
- ☐ User(s) should delete temporary Internet Files and cookies to avoid fraudulent access to "saved" user names and passwords on other sites.
- ☐ Once you have identified the extent of the vulnerability, remove the malware. In certain cases, a computer may need to be replaced.
- ☐ Confirm with your financial institution requirements to verify that the vulnerability has been remedied.
- ☐ Once you can prove either the malware has been removed or the computer has been replaced, ask your financial institution to reinstate access to online banking account and reactivate any other suspended services.

7. Prevent Future instances of Corporate Account Takeover

- ☐ Utilize Best Practices for Businesses on page six to develop policies and procedures to mitigate future instances of corporate account takeover.

If you believe you have been a victim of corporate account takeover, please contact the following bank employees immediately.

Bank Employee Information

Steven LaPierre
Assistant Vice President Cash Management
Work- 781-320-1136 during business hours
Personal Mobile- 508-345-7124

Kerry Riggins
Vice President Digital Banking
Work- 781-320-1455 during business hours
Personal Mobile-781-492-4238

Gina Iantosca
Assistant Vice President Digital Services
Work- 781-320-1160 during business hours
Personal Mobile- 617-775-7034

Tonia Reilly
Senior Vice President Deposit Operations
Work- 781-320-1460 during business hours
Personal Mobile- 781-249-0498

Corporate Account Takeover (CATO)

This guide was created to increase our customers' awareness of the potential risks and threats that are associated with Internet and electronic-based services, and to provide solutions and tools to help prevent fraud and scams.

What is Corporate Account Takeover?

Corporate Account Takeover occurs when a fraudster obtains electronic access to your bank account and conducts unauthorized transactions. The fraudster 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 bill payment 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 businesses. Account takeover can also happen to consumers.

What are methods of *Corporate Account Takeover*?

There are several methods being employed to steal confidential security credentials. *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 fraudster is stealing their security credentials through a fictitious representation which appears to be their financial institution.

A second 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 fraudster 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 fraudster 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 fraudster 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 fraudster can take over the account of the business. To the financial institution, the credentials appear to be the legitimate user. The fraudster 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 fraudster 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 using other popular money transfer services

Fraudsters 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 and Disbursement) debits to other small business accounts for which the fraudster 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.

Fraudsters can also set up and send bill payments through the online banking system.

What are some signs that my online account was compromised?

- Inability of user to login to online banking system (cyber criminals may block access during an attack to distract the user and hide the theft)
- Strange message that the online account is not available
- Sudden request for the user to input password (or security token) in the middle of the online session

(*Contact your financial institution immediately to verify if the system is actually down)*

Signs of a compromised computer network:
(*Contact your IT department immediately)*

- Extreme Loss of performance, including speed and battery life
- Changes in screen appearance, including new apps, icons, toolbars or extensions
- Device suddenly locks up, reboots, or does not allow the user to shut down

- **Administrative changes:**
  - Creation of new online user account(s)
  - New payees added to ACH and Wire transfer templates
  - Changes in payee account and routing numbers
  - Disabling or changing of alerts/notifications
  - Change of address, phone number, or other contact information
- **Unusual user activity:**
  - Login from a different IP address
  - Login and activity at unusual times of the day
  - Password or security token information suddenly not accepted
- **Unusual external transfers:**
  - Small or large amounts being transferred (compared to normal activity)
  - External transfers to new payees (through ACH, Bill Pay, Wire)
  - Overseas transfer(s)

What can business customers do to protect themselves (Best Practices)?

- 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 security tools, including Anti-Virus & Anti- Malware software. Allow for automatic updates and scheduled scans.
- Install firewalls to prevent unauthorized access to your devices or network.
- Change the default passwords on all network devices.
- Install security updates (patches) to device operating systems and all applications as they become available.
- Block Pop-Ups by default and only allow from trusted sources.
- Use strong password policies to ensure passwords are long, strong, and unique across all devices and applications.
- Consider Multi-Factor Authentication (MFA) for applications that send or receive sensitive information.
- Be on the alert for suspicious and unexpected emails. Do not open an attachment or link from a suspicious email and do not reply to the sender.
- Do not use public Internet access points-they are freely accessible to anyone, including cyber criminals.
- Monitor and reconcile Bank Accounts daily - especially near the end of the day.
- Note any changes in the performance of your devices (e.g., extreme loss of speed or battery life, computer lock-ups, unexpected rebooting, unusual pop-ups).
- Make sure that your employees know how and to whom to report suspicious activity – both at your Company & your Bank.
- Use multi-layer security.
- Consider Cyber Insurance

Contact the Bank if you:

- **Suspect a Fraudulent Transaction**
- **If you are trying to process an Online Wire Transfer or ACH Batch and you receive a Maintenance Page**
- **If you receive an email 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, Security Codes or Passwords via e-mail.