Business Incident Response Plan Checklist for Account Takeover

Since each business is unique, clients should develop their own Incident Response Plan. A general template would include the following:

1. Notify your financial institution(s)

- ☐ Review your recent account activity for unexpected/unknown transactions.
- ☐ Request a hold be placed on affected account(s) to stop all activity.
- ☐ Make sure all online banking functions are disabled or suspended.
- ☐ Close affected account(s) and open replacement account(s), if necessary.
- ☐ Change online banking user ID and password.
- ☐ Consider changing user IDs and passwords on other systems.

2. Gather details on the unexpected/unknown transactions and attempt to stop transfers of funds with financial institution(s)

- ☐ Date(s) of incident(s):

  _____
- ☐ Type of transaction involved:

  _____
- ☐ Request assistance from financial institution(s) to stop pending transfers as necessary.
- ☐ Dollar amount, ABA (bank routing number), and account number(s) involved:

  _____
- ☐ How did you discover the incident? Who reported it?

  _____
- ☐ What is the user ID used in the incident?

  _____
- ☐ Was the user ID and/or password shared?

  _____
- ☐ Did the user notice anything unusual during the login process?

  _____
- ☐ Have you confirmed that this activity is fraudulent?

  _____

3. Notify applicable parties at your company

- **Management:** Oversee and coordinate the process.
- **IT Department/Vendor**: Identify and mitigate further attacks.
- **Bookkeeping/ACH Officer**: Work with financial institution(s) on recovery.
- **Corporate Security**: Contact law enforcement.
- **Public Relations**: Work on press release, if needed.
- **Legal Counsel**: Consider and coordinate legal issues.

4. Attempt to recover lost funds and plan for recourse

- ☐ Ask your financial institution(s) for assistance to contact other financial institution(s) involved in incident 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(s).
- ☐ Contact your insurance company and determine what coverage you have on any loss.
- ☐ Alert employees of confirmed or suspected corporate account takeover.
- ☐ File a complaint with the Internet Crime Complaint Center at: https://complaint.ic3.gov/

5. Identify vulnerability and begin a plan to remedy

- ☐ Does the user ID involved in the incident log into more than one computer or through remote access?
- ☐ Is the computer involved in the incident connected to the network?
- ☐ Does the computer involved in the incident have antivirus software installed on it? Is antivirus kept up to date with virus definition updates and periodic scans?
- ☐ When was the last time someone at your company accessed online banking with the user ID involved in the incident? This may help to determine date/time of compromise.
- ☐ What was the potential source of the compromise?
    - Phishing email/text (Identify sender, date/time email was received, attachment/link accessed from the email)
    - Website (Identify website URL, date/time website was accessed, information entered on the website, items accessed on the website)
    - Computer Pop-up (Identify date/time pop-up appeared, summary of pop-up content, action(s) taken because of pop-up)
- ☐ Temporary Internet Files and cookies should be deleted from the computer involved in the incident to avoid persistent access to “saved” user credentials on other sites.
- ☐ Malware should be removed from the computer involved in the incident. In certain cases, a computer may need to be replaced.
- ☐ Confirm with your financial institution(s) requirements to verify that the vulnerability has been remediated.
- ☐ Once you provide remediation verification to your financial institution(s), request the enablement of the user ID involved in the incident and the reactivation of any other suspended services.

6. 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

Ed Skou

Director of Treasury Management
Work: 781.347.6642
Mobile: 617.875.5483

Corporate Account Takeover

This guide was created to increase client awareness of the potential risks and threats that are associated with Internet and electronic-based services, and to provide best practices to help prevent incidents.

What is Corporate Account Takeover?

Corporate Account Takeover (CATO) occurs when a fraudster obtains electronic access to your bank account and conducts unauthorized transactions. The fraudster obtains electronic access by stealing user IDs and passwords of your employees who are authorized to conduct electronic transactions (e.g., wire transfers, Automated Clearing House [ACH], bill payment, and others) on your bank account. Losses can range from thousands to millions of dollars with the majority of losses not fully recovered. CATO has affected both large and small businesses. Account takeover can also happen to consumers.

What are methods of Corporate Account Takeover?

There are several methods fraudsters use to steal account credentials. Phishing emails and websites can impersonate the look and feel of a legitimate financial institution. Users freely provide their credentials within these spoofed emails and websites without knowing that it is being received by fraudsters.

A second method is *Malware* that infects devices via infected emails, websites, or pop-ups. In addition, malware can be downloaded to a user's device from legitimate websites, especially social networking sites. Clicking on unverified ads or links can redirect users to sites that automatically download and install the malware. One specific type of malware used to impact bank clients is called a Banking Trojan. Banking Trojans may appear to be legitimate software, but they are designed to steal online banking credentials and/or gain access to financial information stored on devices.

What does Corporate Account Takeover look like?

If user's online banking credentials are stolen, then the fraudster can access and take over the online banking account and any accounts linked to it. The fraudster can review detailed information, including account activity/patterns and ACH/wire transfer origination parameters (e.g., file size, frequency limits, Standard Entry Class [SEC] codes, etc.).

With an understanding of the permissions and the limits associated with the online banking account, the fraudster can transfer funds out of linked bank accounts 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 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.

Potential Indicators of Compromise

Signs of a compromised online banking account:

(Contact your financial institution immediately to verify if the online banking system is offline or if your account is reporting suspicious behavior)

- ☐ Inability of user to log into online banking system
- ☐ Strange message indicating 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
- ☐ **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)
- ☐ **Signs of a compromised computer and/or 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

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

- Education is Key. Train your employees!
- 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 Antivirus & Antimalware 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 as they are freely accessible to anyone, including fraudsters.
- 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 lockups, 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.
- Consider Cyber Insurance
- Verify any first time or changed beneficiary payment instructions by calling a known phone number (never rely on email replies).
- Watch out for domain look-alikes, invoice anomalies, and urgent payment requests; independently confirm vendor changes.
- Real-time alerts: new user/payee/template, admin/profile changes. Dual control/segregation of duties for ACH/Wire; set per-user and per-transaction limits.
- Do not allow multiple employees to share the same online banking profile.

Contact your bank if you:

- Suspect of a Fraudulent Transaction
- Receive a Maintenance page when trying to process an online wire transfer or ACH batch
- Receive an email claiming to be from your bank and it is requesting personal / Company information

Charlesbridge Group and its affiliates Dedham Savings and South Shore Bank will NEVER ask for sensitive information, such as account numbers, online credentials, or security codes via email.

SOUTH SHORE BANK

Resources for Business Account Holders

The Better Business Bureau's website on Cyber Security
https://www.bbb.org/all/cyber-security-resources

The Small Business Administration's (SBA) website on Strengthening your Cybersecurity
https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

The Federal Trade Commission's (FTC) interactive business guide for protecting your small business:
https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

Account Takeover Fraud from the U.S. Secret Service, FBI, IC3, on the IC3 website
https://www.ic3.gov/CrimeInfo/AccountTakeover

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

Have I Been Pwned? – Online database of known data breaches maintained by security researchers. Check to see if your company email addresses have been potentially compromised.
https://haveibeenpwned.com/