Corporate Account Take Over Guide (CATO)

This guide was created to increase your 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.

OneLocal
Everyday Banking.

Corporate Account Take Over is a fast-growing electronic crime where thieves typically use some form of malware, or malicious software, to obtain login credentials to corporate online banking accounts and fraudulently transfer funds from the accounts. Another means fraudsters commonly employ is phishing, masquerading as a trustworthy entity in an electronic communication or through social engineering to gain access to your sensitive information.

These attacks can result in substantial monetary loss for your company that, often, cannot be recovered. As a bank, we do everything we can to keep your money safe. Unfortunately, our security practices can only go so far to protect your accounts from corporate account takeover. There are some vulnerabilities that can only be addressed from the company side and therefore require that the business implement sound practices with their staff, systems, and offices.

1. How Does CATO Fraud Happen?

CATO attacks do not target the security systems or computers of the financial institutions; instead, these attacks seek to find customers that have the ability to initiate funds transfers from bank accounts using their computers. The goal is to obtain the customer's access codes, (username and password), without the customer's knowledge so they will continue to be active and the crook can perform financial transactions impersonating the customer. A common way this is done is to get the customer/user to click on a link in an email, website or pop-up that installs a malware program on the customer's computer. The malware will secretly record the customer's activity and use a "key-logger" to record the usernames and passwords as they are entered when logging into a banking site. This information is either retrieved by the fraudster using a remote connection opened by the malware or sent to their computer for them to use remotely. They may also compromise the email accounts of the user to send transfer requests from the customer/users email account. Other computer information is also stolen such as security cookies or other information to allow the fraudster to logon to the bank's system to make everything appear to look like they are the actual user.

In some cases, the fraudster may use "social engineering" as the way they get this information. To do this, the fraudster may place a call, send an email, or make a personal visit to the office and claim to be from the bank or another trusted source and request the information as part of a trouble-shooting effort. Often it is done with an email that claims the user must update their account information or confirm a password due to a problem or security alert that appears to be from a financial institution.

Once the fraudster has the customer/user's banking credentials (login and password), they will logon to the banking sites and create transfers using the ACH or Wire Transfer features to steal funds from the accounts tied to the credentials. These methods are the primary ones selected because they can send large amounts of money, and the funds are immediately available for withdrawal when received or on the next day. The money may go straight to the fraudster, but more often it will go to a person that has been recruited to receive the funds and immediately forward the funds to the crooks. The "money-mule" will typically not know they are part of a fraud and usually believe they only responded to an employment or other advertisement on the web that promised they can keep a handling fee. This trick keeps the fraudster's identity and location out of the transaction. Once the money has been withdrawn, recovery is nearly impossible due to the banking rules.

After the discovery of the fraudulent transactions, the business and bank will need to work together to try to recover funds. In most cases, there will be an amount that cannot be recovered and represent a loss to either the customer or financial institution. There are currently no clear rules on who will suffer the loss in these situations. Many losses have been settled on a case-by-case basis depending on the entity that had its security responsibility breached by the compromise. In cases where a company fails to use any of the recommended security procedures offered by the bank or has lax internal security and controls, they have often been held to absorb all, or a portion, of the liability for the loss.

Keep in mind that once a cyber-criminal has successfully taken over control of your online banking account (CATO) they may or may not be looking for a quick payday by transferring funds immediately. In many cases cyber criminals are aware of additional security measures that they cannot by-pass easily, such as physical tokens. With this in mind cyber criminals have observed lingering in your accounts for many months, collecting data on your business, your employees and the entities you pay or collect from in order to commit other types of fraud against you and them, such as identity theft, online purchases, and loan fraud.

2. Sound Business Practices That Can Help Prevent CATO Losses

We have outlined some ideas on areas or tools that can be used to thwart fraudsters that want to attack your business or staff. Although, even if every suggestion or recommendation is adopted by the business; a potential for a user's account to be compromised will still be present. The bank is constantly working to add other security measures on our side to proactively detect suspicious activity or perform other security reviews and out-of-band confirmations prior to allowing the completion of a funds transfer. Here are some security measures we urge you to take to safeguard your business from fraud, they represent a security-in-depth model, and it should be noted that as technology evolves the methods and tools below will need to constantly be updated.

The battle begins with creating a work environment where the staff is aware of the threats posed by using the internet and how it is a doorway into the computer network of the company. Sharing this document can help educate your employees about cybercrimes and other means fraudsters may attempt to gain access to the company's accounts.

It is everyone's job to help keep the computer systems secure from outsiders. Even a laptop or home computer that has remote access to the network can allow hackers access if the user's PC is compromised and has sufficient network rights. Below are some tips that should be shared with the staff:

- **Think!** Before responding to any call or email, first ask yourself: *Does this email or phone call make sense?*
- **Deny!** Never provide your user ID and password to anybody, and even more importantly NEVER disclose a Transaction Authorization Code.
- **Distrust!** Do not trust ANY email, internet site, link or caller unless you know for sure it is legitimate.
- **Conduct Training Sessions and Stay Current:** Hold staff training about the risks and keep up with news articles or fraud awareness updates. Check out our resources for more information.
- **Link Avoidance:** Never click on a link in an email or internet site unless you know for sure it is legitimate.
- **Download Avoidance:** Never approve anything to be loaded on your computer that was downloaded from an email or website unless you specifically went to a trusted site or made the request. *When in doubt, don't allow it!*
- **Auto-Log Off Setting:** Have your PC automatically time-out and require a password or biometric login to reactivate. Don't leave your computer unattended in an unlocked mode. As an added bonus, you can configure screensavers to market your business.
- **Keep passwords private:** Don't share passwords or write them down. Pick passwords that are hard to crack, but easy to remember. Change them on a frequent basis.
- **Limit administrative rights:** Do not let employees install software without prior approval.
- **Password Wallets:** Because we know creating unique complex passwords for every site can be hard, try using a password wallet like LastPass, KeyPass or eWallet.
- **Secure your computer and networks:** Install and maintain firewalls, spam filters, and real-time anti-virus, spyware and malware protection software. Block access to sites that are unnecessary or represent high fraud risk for malware (online gambling, social media, adult entertainment, hacker sites, etc.).
- **Secure and protect mobile devices:** Develop policies and procedures for use of mobile devices that access your corporate data. Include items such as device PINs, remote wipe, encryption, and locking capabilities.
- **Block pop-ups:** Surf the Internet carefully.
- **Be on the alert for suspicious emails.** Do not open email attachments or click on links.
- **Note any changes in the performance of your computer.** Dramatic loss of speed, unexpected rebooting, computer locks up, unusual popups, etc.
- **Initiate ACH and wire transfer payments under dual control.** One person authorizes the creation of the payment file while a second person authorizes the release of the file.
- **Tokens:** Consider using security tokens, (soft or fob), to offer another level of out-of-band authentications which can be required for any funds transfer, ACH, or Wire transaction.
- **Never access bank accounts from public Wi-Fi hotspots:** Airports, coffee shops, etc.

2b. Computer Security

Protecting computers and internal networks from unauthorized access is a challenge; the security plan will differ at each business or customer due to their specific computing needs and structure. Layers of security systems and access rights generally will offer greater protection, but every business should develop and implement a security plan that is designed to prevent and mitigate the risk of CATO. Some of the common elements of a security plan would include many of the items listed below.

- **Network Protection Tools:** These items are used to block unauthorized traffic from entering the internal network, checking for virus/malware and reporting suspicious activity.
  - Firewall (Blocks unauthorized traffic)
  - Security Suites with Anti-Virus Program (identifies potentially malicious programs and quarantines or automatically removes them from the system and set the scans to update and run daily)
  - Anti-Spyware/Malware (related to Anti-Virus detection suite)
  - Drive encryption (makes data on the network unreadable if stolen)
  - Intrusion Detection System (looks for incoming attacks to immediately block & report them)
- **Isolated Banking Computer:** Sometimes it may be possible to limit a PC to only conduct banking activity and not allowing it connections for general web browsing, email and social networking to reduce the threat of being infected.
- **Screensavers:** This will lock unattended computers and require a password to unlock it.
- **Network Rights:** Services, directories, programs and access is controlled to limit a user to only be able to perform tasks or access data that they have a business need to use. Additionally document access rights (virtual and physical) that staff have.
- **CD Drives & Thumb Drive Deactivations:** Disable drives to prevent any program or files to be uploaded or downloaded from the network or PC to these removable data media.
- **Website, Application & Pop-Up Blocking:** The firewall or activity monitoring system can be set to block sites or applications that may represent a greater risk for malware or fraud.
- **Secure Email:** If confidential information is sent using email, there are systems that can encrypt the message so it can only be read by the intended recipient.
- **Conduct a risk assessment:** Risk assessments can identify any security holes that you need to mitigate.
- **Penetration Testing and Vulnerability Scans:** In some cases, a business may have an external consultant test the security of their systems for possible vulnerabilities from the outside or internal workstations.
- **Laptops & Remote Access Security:** Ensure that any PC or device that can access the internal network uses a secure connection. Company laptops may consider encrypting the data drives if confidential information is present.

- **Patch Updates:** Enable automatic updates for operating system patches, browsers, and any third party applications that support automatic updates. For those that don't set regular reminders to visit the vendor's website to check for updates..
- **Use Two-Factor Authentication:** Whenever it is available, it is recommended that you use two factor Authentication. IT is also recommended that you do not register your browser with OneLocal Bank.

2c. Account Security

A key element of the security procedures is the reviewing of activity on your accounts to help detect any unusual, unauthorized or suspicious activity as soon as possible. Statistics show that customers will discover fraud before the bank in over 60% of the cases. Here are some tips on how to help secure your accounts.

- **Review Daily Activity.** Check the account transactions that post on a daily basis to look for anything that is not authorized. If you use Quicken or QuickBooks, consider downloading transactions daily to keep your accounting records up-to-date and quickly identify anything unusual.
- **Reconcile:** Balance the accounts at least monthly and report any errors or unauthorized entries promptly
- **Limit Access:** Only allow staff with a need to access or initiate transactions rights to the account. This can include rights to view the account, deposit into the account or withdraw from the account, and the dollar limits for each type of transaction (Review the staff list and access rights occasionally to make sure they are set properly.) Additionally document access rights (virtual and physical) that staff have.
- **Dual Approval:** Use dual approval for all transactions over a dollar amount that you wish to have a second person authorize.
- **Transaction Authorization Codes:** Do not lose a penny; enforce TAC's for ALL transactions.
- **Alerts:** Enroll in alerts (text and/or emails) to be sent to the appropriate staff for any activity that may represent a greater risk, such as debit cards, ACH originations, Wire transfers, external transfers, maintenance changes or significant balance changes.
- **Record Security:** Shred old statements, checks or other confidential records with account numbers and access information. Consider e-Statements and e-Notices to minimize paper record or mail theft.
- **Positive PAY:** With old school check fraud on the rise, prevent counterfeit and forged checks from clearing the business account. Additional benefits of Positive Pay include reverse positive pay and ACH positive pay.
- **Social Engineering:** Ensure that staff who have access to your online banking accounts receive regular and on-going training to spot phishing emails and suspicious phone calls.

2d. User Security

A key element of the security procedures is the reviewing of activity on your accounts to help detect any unusual, unauthorized or suspicious as soon as possible. Statistics show that customers will discover fraud before the bank in over 60% of the cases. Here are some tips on how to help secure your accounts.

- **Limit Administrative Rights:** Do not use the administrator user credentials for performing day-to-day processing. Additionally document access rights (virtual and physical) that staff have.
- **Never Share User IDs/Passwords**: Issue separate IDs for every staff member and make sure the staff does not share or post the password where others can view or use it.
- **Multi-factor Authentication Logins:** Use a bank that employs systems that use multiple ways to confirm the user's id or authorization, such as OneLocal Bank. To do this it is recommended that you never register your browser.
- **Use Dual Control:** For monetary transactions, require two different users to complete the transaction. One would create the transaction and a different user will be required to approve it before it can be processed.
- **Enroll in Alerts:** Sign up for transaction, debit cards, maintenance and balance alerts to be sent whenever there is activity on the account or user.
- **Keep Contact Information Current:** This is important if the bank needs to contact the user to confirm any suspicious transactions. The cell phone number is very important.
- **Social Engineering:** Ensure that staff who have access to your online banking accounts receive regular and on-going training to spot phishing emails and suspicious phone calls.
- **Use Out-Of-Band Security methods:** Whenever possible, use an out-of-band method to confirm financial transactions initiated over an electronic channel. (Out-Of-Band means that a confirmation is performed using a different method from how the transaction was created. For example, if a computer was used to create a transaction via an Internet Banking site, a cell phone call would be placed to the user to confirm they submitted the transaction.)
- **Require strong passwords:** This is a basic security recommendation for any user. To keep your logins protected your password should change at least every 90 days and should not be the same as one used for another site or service. To help manage all of your complex user names and passwords we recommend using a password wallet.
- **Limit Account Access and Right Reviews:** Only give rights that the user needs to perform their duties, record their rights, and review them to determine if changes are needed (Remember it is always better to provide too few rights than too many).

2e. Detection And Response

Time is money! This is especially true with a CATO attack because the sooner the fraud is detected and reported, the greater chance to stop future losses and potentially recover funds that may have been taken. The steps listed in the prior sections will enhance the security procedures that should help stop or detect suspicious or unauthorized activity quickly.

If you suspect or identify an unauthorized transaction has been attempted or completed, **NOTIFY US IMMEDIATELY!** Call us at (781) 762-1800 and ask for Deposit Services; they will gather information, block user access and get our fraud department engaged. If you feel your PC has been compromised, turn it off or disconnect it from the Internet immediately to block further access by the hacker. We will work with your staff to monitor your accounts and determine the source of the security breach. We do have additional resources that are available if you find yourself in this situation and we will provide them upon request.

3. Take The Test – Fraud Awareness Self-Assessment

OneLocal Bank is concerned about your privacy and security regarding your confidential financial information. This worksheet is provided as a tool to evaluate the risks and security issues related to certain activities or behaviors in your daily life.

All the answers should be *Yes*, and any *No* answers indicate that you may be at a greater risk for an attempted or successful fraud attack. If you have any questions about the security of your accounts at the bank, please contact any of our customer service representatives.

	Yes	No
Your computers have anti-virus, spyware and malware protection software that is updated regularly with scheduled scans performed at least on a weekly basis. Your operating systems, web-browsers and third party applications are also updated with the latest patches, and you have activated your personal firewall. *If No, install and update these critical software tools regularly from legitimate sources.*	□	□
When using social media, you do not include personal information such as your physical address, phone number or date of birth including the year. Additionally, you do not list any additional confidential information such as the city where you were born, your mother's maiden name, or Social Security Number on websites or comments. *If No, remove this information from your profiles or comments.*	□	□
You use different passwords for your various systems and sites which do not include easily guessable words or identifiable traits such as your birthday, name of a family member, or pet. Your passwords are not less than 5 characters and at least 2 of the characters are a number, special symbol and/or Capital letter. *If No, change your passwords. We recommend that you change them every 90 days.*	□	□
When using email, you never include confidential information about your financial accounts or other information that could provide access to your banking accounts. This would include your account numbers, bank name, login IDs, passwords and other confidential information. You do not click on links in emails unless you are sure they are from a legitimate or trusted source. *If No, stop including this information – email is insecure and can be intercepted.*	□	□
When discarding statements or other documents that contain confidential information, you always shred the document or obliterate the information that is confidential. This information typically is the account number, name, address, bank or other identifying data that could be used to allow unauthorized access or an account takeover. *If No, start shredding or masking data – dumpster diving is a big ID theft threat.*	□	□
You reconcile your monthly statements and report any discrepancy or suspicious activity immediately. You receive e-Statements to reduce the risk of mail theft. *If No, review transactions and balance statements monthly; request e-Statements.*	□	□
You have set up transaction and balance alerts on your debit cards or deposit accounts to warn you when transactions are completed or if the balance changes significantly. You also have configured alerts for user account or maintenance changes. *If No, contact us to set up alerts as necessary to monitor activity.*	□	□

Answering "Yes" to all these questions will not guarantee that you will not be a victim of fraud, but it should lower your exposure to many of the common threats and risks in the marketplace.

4. Explanation Of Potential Liability

Companies are expected to employ reasonable security procedures when conducting financial transactions. CATO frauds typically target security lapses at the business, access device (PC, email, mobile phone) or user level. In most cases, the bank is not in a position to control or dictate what security policies or procedures are actually used by the business or customer when conduction their banking electronically. As mentioned before, if a loss occurs, the business/customer may be held liable for the portion of the loss that can be attributed to their failure to use reasonable care and security procedures as recommended by the bank. The amount of loss can be sizable and therefore requires that the business take appropriate measures to incorporate the security procedures that are recommended and available as long as they do not result in unreasonable demands on the business or user.

If a CATO loss does occur, the bank will work with our customers to seek the most appropriate resolution to the situation. If the bank fails to perform our fiduciary duties in accordance to industry standards, we generally will assume all or some of the liability. We will follow all applicable laws and regulations when dealing with a CATO incident.

5. Other Resources

OneLocal Bank has developed other resource guides that are available to describe our security systems, services and optional security tools that we offer to our customers. These are located on our website or can be requested from our staff. Below are some resources that may provide other helpful information for your business or staff related to frauds and security.

Current eScams and Fraud

Federal Trade Commission (FTC) Business Guide for Protecting Data

Fraud Advisory for Business Corporate Account Takeover
joint issued by US> Secret Service, FBI, IC3 and the FS-ISAC

NACHA – Sound Business Practices for Companies to Mitigate Account Takeover