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 on your corporate bank account.

Cyber thieves can also target employees through phishing, phone calls, and even social networks. It is common for thieves to send emails posing as a bank, delivery companies, court or the Better Business Bureau. Once the email is opened, malware is loaded on the computer which then records login credentials and pass codes and reports them back to the criminals.

How are confidential security credentials stolen?
There are several methods being employed to steal confidential security credentials. One is to mimic the look and feel of a legitimate financial institution's website. Users provide their credentials to these sites without knowing that a perpetrator is stealing their security credentials through a fictitious website which appears to be their financial institution.

A second method is malware that infects computer workstations and laptops via infected emails with links or document attachments. In addition, malware can be downloaded to a user's workstation and 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, including 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 business customers do to protect themselves (best practices)?
Business customers can take many steps to protect themselves against account takeover:

- One of the most effective, yet basic, controls is for business customers to always initiate ACH and wire transfer payments under dual control. For example, one individual initiates the creation of the payment file, and another approves the file for release.
- Using multiple factors to prove identity is very effective in preventing a successful attack. Multiple factors are more challenging to compromise. For example, the use of something the person knows (user ID, PIN, Password) can substantially reduce the vulnerability to an attack.
- Restrict functions that authorized employees may perform to specific computer workstations and laptops that are used solely for online banking and payments. This will help prevent the inadvertent downloading of malware or other viruses by users.
- Ensure that your company's operating system and its components are up to date with current software patches. For example, the use of the most current firewalls, malicious code filtering, virus protection and spyware removal software will aid in the control of network intrusion tactics.
- Business customers should reconcile their bank accounts daily. Many business customers, particularly small businesses, may not typically reconcile their bank account on a daily basis, and therefore may not recognize fraudulent activity until it is too late to take action. Electronic Funds Transfer Act (Regulation "E") is a consumer regulation and does not protect business clients from fraudulent electronic funds transfers (EFT's).
- Business customers should train all staff who interact with the online banking system on corporate account takeover.
- Business customers should consider completing a risk assessment and controls evaluation periodically to mitigate any risk findings.
- Business customers should keep an updated list of their users.

Additional Advisories:

Click on link to download pdf document below.
Texas Bankers ECTF Corporate Account Takeover Recommendations
American Bankers Association's website (ABA)

Sound Business Practices for Companies to Mitigate Corporate Account Takeover:
This document was created by the National Automated Clearing House Association (NACHA) to help companies mitigate the risk of corporate account takeover. The document was developed for companies of all sizes and outlines business processes to consider when reviewing and implementing security procedures.
https://www.nacha.org/userfiles/File/Sound%20Business%20PracticesBusinessesFinal042811.pdf

Icon Bank will NOT contact clients via email requesting electronic banking credentials to your account or request personal information.

In the event of fraudulent or suspicious activity please contact Icon Bank at 281-517-2400.