WHAT IS CORPORATE ACCOUNT TAKEOVER?

Corporate Account Takeover is an evolving electronic crime typically involving the exploitation of businesses of all sizes, especially those with limited to no computer safeguards and minimal or no disbursement controls for use with their bank's online business banking system. These businesses are vulnerable to theft when cyber thieves gain access to its computer system to steal confidential banking information in order to impersonate the business and send unauthorized wire and ACH transactions to accounts controlled by the thieves. Municipalities, school districts, large non-profit organizations, corporate businesses, and any customers that perform electronic transfers are potential targets. 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. These thefts have affected both large and small banks.

This type of cyber-crime is a technologically advanced form of electronic theft. Malicious software, which is available over the Internet, automates many elements of the crime including circumventing one time passwords, authentication tokens, and other forms of multi-factor authentication. **Customer awareness** of online threats and education about common account takeover methods are helpful measures to protect against these threats. However, due to the dependence of banks on sound computer and disbursement controls of its customers, there is no single measure to stop these thefts entirely. **Multiple controls or a "layered security" approach is required.**

Account holders should be the most vigilant in monitoring account activity. They have the ability to detect anomalies or potential fraud prior to or early into an electronic robbery.

Business account holders should be alert for the same red flags related to computer and network anomalies as bank employees. Warning signs visible to a business or consumer customer that their system/network may have compromised include:

1. Inability to log into online banking (thieves could be blocking customer access so the customer won't see the theft until the criminals have control of the money);
2. Dramatic loss of computer speed;
3. Changes in the way things appear on the screen;
4. Computer locks up so the user is unable to perform any functions;
5. Unexpected rebooting or restarting of the computer;
6. Unexpected request for a one time password (or token) in the middle of an online session;
7. Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (system unavailable, down for maintenance, etc.);
8. New or unexpected toolbars and/or icons; and
9. Inability to shut down or restart the computer.