

Warning Signs of Corporate Account Takeover

As part of education for business employees, it is critical that they are educated on the warning signs that a corporate account takeover is in progress. The following “red flags” should be considered as warning signs of a possible attack and investigated immediately.

Online banking administrative changes including:

- 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 online banking user activity including:

- Log-in from a different IP address
- Log-in and activity at unusual times of the day
- Password or security token information suddenly not accepted
- Unusual external transfer activity including:
 - Small or large amounts being transferred (compared to normal activity)
 - External transfers to new payees (through ACH, Bill Pay, Wire)
 - Overseas transfer(s)

The following could be signs of compromised online banking system (*contact financial institution immediately to verify*):

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

The following could be signs of compromised computer network:

- Loss of computer speed
- Changes in screen appearance, including new toolbars or icons
- Computer suddenly locks up, reboots, or does not allow the user to shut down