Member FDIC

BEST PRACTICES FOR COMMERCIAL CLIENTS TO PROTECT AGAINST FRAUD

1. Monitor accounts frequently (daily as a best practice). Immediately review Wire, ACH, or other transaction confirmations.

2. Implement dual controls and approval for ACH and Wire transfers so that dual approval is required before the transaction is initiated at the Originating Depository Financial Institution.

3. Never share user IDs, passwords, or PIN numbers, with anyone. Do not leave them in an area that is not locked/secured.

4. Do not use the same login or password on any other website or software.

5. Obtain and install endpoint protection (antivirus, anti-malware, anti-spyware, and firewall software) and ensure it is active and automatically updated by the vendor or take necessary steps to keep it updated.

6. Consider a dedicated computer for online banking that is never used for e-mail or general internet browsing/surfing.

7. Educate all company personnel on good cyber security practices, clearing the Internet browser's cache before and after visiting the Financial Institution's website, to avoid having malware installed on a computer.

8. If a media player needs to be updated, go to the official media player website to install the update. Clicking on a fake update installation link could mask a hacker downloading malware onto the computer.

9. Verify use of a secure session ("https://" and not http://"). Ensure no error messages are displayed and the address bar turns green.

10. Avoid saving passwords to a computer.

11. Never leave a computer unattended when using any online banking service, and always lock your computer when away.

12. Never access the Financial Institution's website for online banking (or any privileged or sensitive computer system) from a public computer at a hotel/motel, library, coffee house or other public wireless access point.

13. Be suspicious of any employment position that requires use of a personal account for business purposes. Such offers for employment as a mystery shopper, payment processor, etc. where you are required to use you personal account for someone else's business purposes, are not legitimate. No legitimate business will attempt to move business funds through anyone's personal account. If you are approached to participate in such schemes, immediately contact local law enforcement, the FBI or the Secret Service to let them know.