24 Tips to Avoid ACH Fraud

Customer Best Practices:

Among the recommendations for corporate customers to secure computer systems:

- If possible, and in particular for customers that do high value or large numbers of online transactions, carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.
- Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack their computer.
- Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
- Create a strong password with at least 10 characters that includes a combination of mixed case letters, numbers and special characters.
- Prohibit the use of "shared" usernames and passwords for online banking systems.
- Use a different password for each website that is accessed.
- Change the password a few times each year.
- Never share username and password information for Online Services with third-party providers.
- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Ensure virus protection and security software are updated regularly.
- Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
- Consider installing spyware detection programs.
- Clear the browser cache before starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.
- Verify use of a secure session (https not http) in the browser for all online banking.
- Avoid using an automatic login features that save usernames and passwords for online banking.
- Never leave a computer unattended while using any online banking or investing service.
- Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.
- Customers must familiarize themselves with the institution's account agreement and with the customer's liability for fraud under the agreement and the Uniform Commercial Code as adopted in the jurisdiction.
- Stay in touch with other businesses to share information regarding suspected fraud activity.
- Immediately escalate any suspicious transactions to the financial institution particularly, ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by the customer.