Online Banking (OLB) Fraud Prevention Best Practices – For End Users

General Internet Guidelines

- Be suspicious of e-mails purporting to be from a financial institution, government department or any 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 e-mails could expose your system to malicious code that could hijack your computer.
- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail:
  - Call the purported source if you are unsure who sent the e-mail.
  - If an e-mail claiming to be from your bank seems suspicious, checking with your financial institution.
- Never provide sensitive or personal information in response to an e-mail message, even if it appears to be from your financial institution. If you are uncertain whether they have actually requested this information, contact them by telephone.
- Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.
- Install anti-virus and spyware detection software on all of your computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Check your settings and select at least a medium level of security for your browsers.
- Ensure virus protection and security software are updated regularly.
- Never share username and password information with third-party providers.
- Ensure computers are patched regularly, particularly operating systems and key applications, with security patches.
- Do not use account numbers, social security number (SSN) or other account or personal information when creating account nicknames or other titles.
- Whenever possible, register your computer to avoid having to re-enter challenge questions and other authentication information with each login.
- Do not open e-mail from unknown sources.

Tips for Wireless Network Management

Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended wireless networks are secured as follows:

- Change the wireless network hardware (router /access point) administrative password from the factory default to a complex password. Make certain to save the password in a secure location as it will be needed to make future changes to the device.
- Disable remote administration of the wireless network hardware (router/access point).
- If possible, disable broadcasting the network service set identifier (SSID).
- If your device offers Wi-Fi Protected Access (WPA) encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable Wired Equivalent Piracy (WEP) encryption.

- If only known computers will access the wireless network, consider enabling media access control (MAC) filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering only allows computers with permitted MAC addresses access to the wireless network.

For OLB Cash Management Users

General Guidelines for Online Banking Activity

- 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 depends on the browser and version you are using. This function is generally found in the browser's preferences menu.
- Do not use public or other unsecured computers for logging into Online Banking.
- Avoid using automatic login features that save usernames and passwords for online banking.
- Never leave a computer unattended while using online banking.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Create a strong password with at least eight characters that includes a combination of mixed case letters, numbers, and special characters.
- Change your password frequently.
- Always check the last login date/time every time you log in.
- Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.
- Review account balances and transaction details regularly (preferable daily) and immediately report any suspicious transactions to your Financial Institution.
- Take advantage of automated alerts; examples include:
  - Passwords are changed
  - E-mail addresses are changed
  - Balance exceeds or drops below a certain level
  - Weekly and daily available balance
  - Monetary transactions such as fund transfers or stop payments are processed or cancelled
- Whenever possible, use Bill Pay in lieu of checks to limit account number dissemination exposure and to obtain better electronic record keeping.

Administrative Users

- Limit administrative rights on users' workstations to help prevent inadvertently downloading malware or other viruses.

Online Banking (OLB) Fraud Prevention Best Practices – For End Users

- Dedicate and limit the number of computers used to complete online banking transactions; allow no Internet browsing or e-mail exchange and ensure these computers are equipped with the latest versions and patches of both anti-virus and anti-spyware software.
- Delete online user IDs as part of the exit procedure when employees leave the company.
- Assign dual system administrators for online cash management services and require secondary approval for Automated Clearing House (ACH) Batches and wire transfers.
- Establish transaction dollar limits for employees who initiate and approve online payments.
- Require additional Security Token entry for users responsible for monetary transactions such as account transfers, ACH batch entries and approvals and wire transfer entries and approvals.
- Manage access for each user only to the specific services that a user is required to access to do their job.

Tips to Protect Online Payments and Account Data

- Take advantage of transaction limits. Establish limits for monetary transactions at multiple levels – per transaction, daily, weekly or monthly limits.
- When you have completed a bank transaction, make certain to log off to break the connection with the bank's computer.
- Use separate accounts for electronic and paper transactions to simplify monitoring and tracking any discrepancies.
- Reconcile by carefully monitoring account activity and reviewing all transactions initiated by your company on a daily basis.

ACH Batches

- Utilize pre-notification transactions to verify account numbers within your ACH transactions are correct.
- Utilize limits for monetary transactions at multiple levels – per batch, daily, weekly, or monthly limits.
- Review transaction reporting regularly to confirm transaction activity.
- Utilize available alerts for ACH activity.

Wire Transfer

- Utilize limits provided for monetary transactions at multiple levels – per transaction, daily, weekly, or monthly limits.
- Review historical and audit reports regularly to confirm transaction activity.
- Utilize available alerts for wire transfer activity.

Account Transfer

- Utilize limits provided monetary transactions at multiple levels – per transaction, daily, weekly or monthly limits.
- Review historical and audit reports regularly to confirm transaction activity.

Online Banking (OLB) Fraud Prevention Best Practices – For End Users

- Utilize available alerts for funds transfer activity.