COMMERCIAL BANK

Online Banking Fraud Prevention Best Practices

This document provides you with fraud prevention best practices.

User ID and Password Guidelines

- Create a “strong” password with at least 8 characters that includes a combination of mixed case letters, numbers, and special characters.
- Change your password frequently.
- Never share username and password information with third-party providers.
- Avoid using an automatic login feature that saves usernames and passwords.

General Guidelines

- Do not use public or other unsecured computers for logging into Online Banking.
- Check your last login date/time every time you log in.
- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to your financial institution.
- View transfer history available through viewing account activity information.

- Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping.

- Take advantage of and regularly view system alerts; examples include:
    - Balance alerts
    - Transfer alerts
    - Password change alerts
    - ACH Alerts (for cash management users)

- Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.

- Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.

- Never leave a computer unattended while using Online Banking.

- Never conduct banking transactions while multiple browsers are open on your computer.

- An FBI recommended best practice is to suggest that company users dedicate a PC solely for financial transactions (e.g., no web browsing, emails, or social media).

Tips to Protect Online Payments & 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 transaction, ensure you log off to close the connection with the financial organization'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.

Account Transfer

- Use 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 funds transfer activity.

Below are specific guidelines for businesses using Online Banking cash management functionalities

ACH (Automated Clearing House Batches)

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

Administrative Users

- Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
- Dedicate and limit the number of computers used to complete online banking transactions; do not allow Internet browsing or e-mail exchange and ensure these computers are equipped with 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 your company.
- Assign dual system administrators for online cash management services.
- Use multiple approvals for monetary transactions and require separate entry and approval users.
- Establish transaction dollar limits for employees who initiate and approve online payments such as ACH batches, wire transfers, and account transfers.

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. 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 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 an e-mail.

- If an e-mail claiming to be from your financial organization seems suspicious, checking with your financial organization may be appropriate.

- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.

- Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.

- Ensure computers are patched regularly, particularly operating system and key application with security patches.

- 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.

- Check your settings and select, at least, a medium level of security for your browsers.

- 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.

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 that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router /access point) administrative password from the factory default to a complex password. 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 SSID.
- If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption.
- If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.