Best Practices: General Internet Security

- **Secure Location:** Position those computers used to transact business in a secure location. Try to keep computers away from public areas and beware of opportunities for "shoulder surfing" where unauthorized persons might view transactional activity on a computer screen.

- **Time-Out:** Utilize the "time-out" feature available for your browser. Set the screen to revert to a screensaver after a specified number of minutes of inactivity and require a password to log back in. Never leave computers unattended while using any type of online banking services.

- **Browsers:** Always sign-out when finished using any online application and then close the browser. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser. Use the most current version of a recommended browser that supports Secure Sockets Layer (SSL) protocol and 128-bit encryption. Apply any updates to your desktop operating system and your browser as often as they are made available.

- **Encrypted Applications:** When using applications that require login credentials and/or process sensitive data, always ensure "https:/" (an "s" after the "p" not "http:/") is in the address bar just prior to the website address.

- **Anti-Virus & Anti-Spyware:** Install and use anti-virus, firewall, and anti-spyware programs. Ensure your anti-virus receives daily updates. Install new security patches as soon as your operating system and Internet browser manufacturers make them available.

- **Email Security:** Automate scanning of attachments within email. Implement Spam Filtering on inbound email to block unsolicited email that may contain malicious URLs. Spam Filtering should validate that the sender has a valid email address and comes from a valid domain name before delivering the email to your users' inboxes. Always beware of email asking for personal or login information. Although fraudulent email can be difficult to recognize, beware of emails that:

  1. Request that you click a link which could take you to a spoof website - one that looks like a real company website and may even include the real company's official graphics and design. Phishing email has been known to impersonate companies such as NACHA, FedEx, the IRS and the Federal Reserve. Since a fraudulent email may even use exact wording from the real company's website, it can be difficult to identify a spoof website.
  2. Ask you to give, confirm, or update sensitive personal information, such as Social Security numbers, usernames, passwords, PIN numbers, or account numbers. NOTE: Even if you don't enter your personal data, by clicking on a link embedded in a fraudulent email, you may inadvertently download tracking software or viruses that track your keystrokes to gain your personal information. The Bank will not ask you to enter (or record) personal or account information via email.
  3. Use pop-up windows for entering or confirming personal data.
  4. Have a sense of urgency asking you to provide the information immediately, citing a specific event that might happen if you fail to respond. For example, the email may state that your account may be closed or temporarily suspended.
  5. Contain spelling errors and/or bad grammar. Intentional spelling errors may allow the email to bypass spam filters used by Internet Service Providers (ISPs).

  If you receive one of these email messages, do **not** open any attachments or click on any links in the email. These emails are not authentic and the links may contain Trojans which could jeopardize your online banking.

- **Password Protection:** Maintain strict confidentiality of IDs, passwords, PINS, and (if applicable) token. The Bank will never request your login credentials for any reason, whether through email, via phone, or other method. Don't share or post IDs, passwords, or PINs or use "guessable" IDs, passwords, or PINs. Disable automatic password-save features in the browsers and software you use to access the Internet. We also recommend you set a reminder to change your passwords periodically, and that you use a unique password for each website.

- Mobile Devices: Mobile devices are becoming more frequent targets of cyber criminals. The following are best practices when conducting financial transactions from a mobile device.
    - Conduct business financial transactions from devices that are in compliance with your organization's security policies, enforced through an enterprise mobile device management solution.
    - **Never** access bank accounts from cafés or public Wi-Fi hotspots, or hotspots not controlled by you.
    - Do not circumvent security features or otherwise "jailbreak" your mobile device.
    - Ensure encryption is turned on for your mobile device.
    - Keep your mobile devices with you at all times or store them in a secured location when not in use.
    - Mobile devices should be password protected and auto lockout should be enabled. The password should block all access to the device until a valid password is enabled.
    - Ensure your device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible.
    - Wireless access, such as Bluetooth, Wi-Fi, etc., to the mobile device should be disabled when not in use to prevent un authorized wireless access to the device.
    - Only download applications from trusted App Stores.
    - Wipe or securely delete data from your mobile device before you dispose of it.