Online Banking Fraud Prevention Best Practices

General Safety Tips

User ID and Password Guidelines

- Create a “strong” password using at least 8 characters that are a combination of:
  - Mixed case letters (“A”, “a”)
  - Numbers (0 – 9)
  - Special characters (!, @, #, $, %, ^, &, *, ?)
- Change your password frequently
- Never share your password with ANYONE. If you suspect misuse, please call us.
- The Bank employees or representatives will NEVER ask you for your password by e-mail. If you receive a suspicious “phishing” e-mail from the Bank please call us.
- Avoid using the automatic function in web browsers to store a username and password

General Guidelines

- Do not use public or other unsecured computers to log into your Online Banking.
- Check the Last Logon Date and Time every time you log in.
- Review your account balances and transaction history regularly to confirm payment and other transaction data.
- Immediately report any suspicious transactions.
- Reconcile check and Bill Pay transactions to maintain better electronic record keeping.
- Do not use account numbers, SSN/TIN numbers, or other personal information when creating account nicknames or other titles.
- When using non-public computers, register the computer to avoid having to re-enter challenge questions and other authentication information with each login.
- NEVER leave a computer unattended when performing Online Banking transactions.
- NEVER perform banking transactions while multiple browsers are open on your computer.

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.
- Never respond to suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail.
- Install and update anti-virus and spyware detection software on all computer systems.
- Ensure computers are patched regularly, particularly operating systems and key applications.

- Install a dedicated, actively managed firewall, especially if you are 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 browser settings and select, at least, a medium level of security.
- Be advised that the Bank will never present you with a maintenance page after entering your login credentials. Legitimate maintenance pages are displayed when first reaching the site and before entering login credentials.
- Online Banking does not use pop-up windows to display login messages, errors or notifications of browser usage. All messages will be displayed directly on the login screen and will never include an amount of time to wait before attempting to log in again.
- If you are asked to repeatedly re-enter your password/token, or unexpectedly answer your challenge questions could be signs of potentially harmful activity.

Online Banking Administrative Users and Cash Management Transactions

- Prohibit the use of "shared" usernames and passwords
- Limit administrative rights on users' workstations to help prevent inadvertent downloading of malware or other viruses.
- Dedicate and limit the computers used to complete Online Banking transactions. Limit Internet browsing and e-mail use on these computers and ensure these computers are equipped with the latest versions and patches of both anti-virus and anti-spyware software.
- Manage 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 money 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.
- Use pre-notification transactions to verify that account numbers within your ACH payments are correct.
- 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.

If you have any questions please call us @ 662-252-4211 or 662-252-1341