TRI CITY NATIONAL BANK

Your Hometown Bank

Business Online Banking - Fraud Prevention Best Practices

This document is being provided to you, our Business Customer, as a tool to help protect your organization from fraud or potential loss.

SECURING YOUR COMPUTER

- Keep virus protection, antivirus, anti-spyware and operating systems up to date by electing automatic updates when patches are available.
- Wireless networks are not recommended without enhanced security.
- If practical, use a dedicated computer for all online banking transactions.
- Always lock your computer when you leave it unattended. In Windows use the Ctrl-Alt-Del function. You can also use the automatic screen lock feature, if available, after a set period of inactivity, e.g. 15 minutes. If using Windows, this feature can be found in your display properties.
- Verify use of secure session (https:\\ not http:\\) in the address bar of your browser when logged into online banking.
- Clear the browser history after each Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the history is cleared will depend on whether you use Internet Explorer or other versions. This function is generally found in the 'Internet Options' menu.
- Be suspicious of emails and text messages claiming to be from a bank, government department or other agency requesting account information.
- Never use a link within an email to access online banking. Type the bank's website address directly into the Internet browser: www.tcnb.com
- Immediately report any suspicious activity in your account. There is a limited recovery window and a rapid response may prevent additional losses.
- Review educational materials that can be found on the web site at: www.tcnb.com
- If the computer knowledge or resources are unavailable within your business it is recommended that you utilize a security expert to run security software and test your network for known vulnerabilities.

ADMINISTRATION

- Administrator account is only to be used to add and remove users.
- On a periodic basis verify existing users are limited to only needed access.
- Setup profiles to reflect needed user functionality and ACH collection/payment limits.
- Establish separation of duties within your business. Example: limit one user to setup or run transactions through ACH or Bill Pay and one user to transmit.

Tri City National Bank, P.O. Box 44017 West Allis, WI 53214

- Include in your employee termination policy steps regarding the immediate removal of access from terminated employees.

LOG IN

- Each time you log in confirm last sign on date on the Business Online Banking (TriDATA) Welcome page.
- Do not use account numbers when providing nicknames for the account.
- Create strong passwords. Current minimum requirements are:
    - 8 – 12 characters with at least 1 number and 1 Uppercase letter. To strengthen the minimum requirements use at least 1 symbol.
    - Do not use this password for other systems.
- Avoid using an automatic login feature that saves username and passwords for online banking.
- Limit where you login, never login on a public or unsecured computer (e.g. library or hotel, internet café, your home).
- Prohibit the use of "shared" userIDs and passwords for online banking systems.
- Use a different password for each website that is accessed and change the password frequently.
- Setup and view alerts and notify us if you don't recognize the activity.
  Alerts should be setup for the following:
    - When a password is changed.
    - When a sub-user's role is changed (e.g. when someone is given the approval or administrative role)
    - When an email address is changed.

ACH / FILE UPLOAD

- Review ACH history on a regular basis.
- Multiple approvals should be used to send ACH transactions.
- Use alerts for ACH transactions. Alerts should be setup for the following:
    - Notify you that an ACH template has been modified.
    - If ACH transmission needs approval.

OTHER TRIDATA FUNCTIONALITY

- *Wire*: Verify wire history.

- *Funds Transfers*: verify funds transfer history.

- *Business Bill Payment:* Verify bill payment history reports on a regular basis.