TMS Safety Controls

With advancing technology comes new ways for potential scammers to find weaknesses to launch cyber attacks on businesses. At Jefferson Bank, we appreciate your trust in meeting your business transaction needs and look for ways to keep your finances protected.

With our Treasury Management Services, we offer security controls to help keep your business cyber-safe. Talk with our Treasury Management Specialists to make sure you are taking advantage of these safeguards.

- **Virtual Tokens** - digital security devices that allow only authorized Users to transmit ACH/Wire transactions. Virtual tokens are an additional security layer added to passwords. Employees with access to their own security token should only use their own and not share it with other Users.
- **Detect Safe Browsing (DSB)** - software tool that provides a safe browsing experience and blocks the execution of malicious software to ensure a Secure Online Banking session.
- **Device Registration** - links the User's device (PC or Mobile) to the Online Banking system. If the device is not registered, the system will decline access or activate additional security authentication.

- **Alerts** - offered by Email or SMS Text Alert to monitor monetary transactions and to prevent unauthorized transaction activity. With Alerts, Business Owners or Administrators are always aware of monetary transactions processed by their staff. The following Alerts are recommended to be activated prior to submitting ACH or Wire Transactions.
  - Address is changed.
  - Outgoing ACH transactions are created.
  - Recipient is added.
  - Wire transfer (International and/or Domestic) is created.
  - New computer/browser is successfully registered.
  - Payment template is created.
  - New user role is created.
  - Invalid password for my login ID is submitted.

Have confidence knowing your account is guarded with the following system-related settings:

- **Dual Control** - required security control in which one User drafts the ACH/Wire transaction and a second User Approves the transactions for processing.
- **Processing Limits** - established to allow ACH/Wire transactions to process within your normal cash flow range.
- **Account Number Lock Down** - controls which Jefferson accounts will be used for processing ACH/Wire transactions.
- **Real Time Fraud Anomaly Detection for ACH/Wire Transactions** - an anomaly detection software utilized to monitor and track variations in Internet Protocol (IP) Addresses, New Recipients, and Batch Amounts/Counts, Dates/Time of processing, and PC/Mobile device used to process transactions.
- **Geo Location** - limits the ability to draft ACH/Wires transactions to IP Addresses within the United States and/or Internationally.
- **IP Restrict** - limits the ability to draft ACH/Wires transactions to IP Addresses designated by the customer.
- **Date/Time Draft Management** - assist with restricting processing dates and times to prevent unauthorized activity.

JEFFERSON BANK

MEMBER FDIC

Extra protection with Positive Pay

One of the Treasury Management Services we offer called Positive Pay, is a fraud prevention tool that detects any unauthorized Checks and ACH transactions attempting to pay against your bank account. Ask a Treasury Management Specialist for more information about this service that is offered at an additional cost.

How you can protect yourself

There are ways you can help keep your computer system and network protected from cyber attacks even if you're not an internet guru. Use this checklist to help protect your business.

- Install, use and keep up-to-date anti-virus/spyware on business computers and network.
- Utilize automatic and scheduled scans for anti-virus and anti-spyware.
- Install, use, and keep an updated firewall on each computer and network.
- Utilize the latest versions of approved web browsers and keep your computer, operating system and software up to date.
- Restrict staff from accessing social networks which are prone to malware attacks.
- Restrict staff access from unauthorized web downloads, changes to the firewall, or ability to alter system settings designed to deter malware.
- Turn off the auto-fill feature on web browser to avoid recall of user login information.
- Monitor employees' use of DVD/CD-ROM & USB drives and installing software.
- Keep the computer used for Online Banking services located in a secured area away from public view.
- Require passwords to log on to your company computers and network and enforce employees to follow safe password guidelines to include:
  - Using their own passwords, which are private and not shared with others.
  - Creating complex and unique passwords that are not also used on any other website or platform.

For added protection, consider contacting an IT Security or Network Specialist to ensure systems are operating securely.

If you have questions or concerns, please contact:

Treasury Management Support
(210) 736-7206
treasurysupport@jeffersonbank.com

JEFFERSON BANK
JeffersonBank.com