Fraud Prevention.

Tips to help protect your business.

How well-protected is your business?

The risk of fraud is always present. While you can't predict when or how your business may be targeted, there are many steps you can take to reduce the chances of a fraud attempt becoming a fraud loss.[1]

We've collected helpful tips that our customers have implemented as a source of ideas to develop or enhance your own fraud prevention plan. You will see that many of these practices can be implemented easily and inexpensively.

Whatever you do, don't wait until your business suffers a loss to realize that fraud can be prevented. Now is the best time to take action to better protect your business.

Review your accounting and reconcilement

- Segregate reconcilement duties from payment initiation functions
- Reconcile accounts daily
- Validate requests from vendors to modify payment instructions before making changes
- Use separate bank accounts to isolate transaction types (i.e., deposits versus outgoing wires or checks issued)
- Obtain a full audit by an accounting professional that includes a complete review of your security procedures

See reverse side for more information.

Quick tips

Online banking

- Limit user access to match job duties
- Use dollar limits and secondary approvals per transaction or per day
- Create wire and ACH templates, and allow users to create only template payments
- Verify the legitimacy of the source for non-repetitive wire and ACH payments prior to release
- Use alerts to notify you of significant balance changes or payments processed

Safe computing

- Prohibit the use of shared user names and passwords
- Disable auto complete and similar password storage functions on web browsers
- Never access online banking from a public computer or Wi-Fi
- Inform employees of the dangers of clicking links or opening attachments in e-mails from unknown senders
- Instruct employees on what to do if they suspect a PC or network compromise

[1] Losses suffered as a result of cybercrimes may not be covered under general liability insurance. Please consult with your insurance professional about cyber liability coverage.

TD Bank

America's Most Convenient Bank®

Partner with your technology experts

Do employees know what your anti-virus software protects against versus what it does not? Are your applications configured in ways that help deter fraud, like receiving e-mails as plain text or flagging messages with extensions similar to the company e-mail? Take advantage of the expertise offered by technology partners to answer questions such as these and to guide you in choosing the right tools and configurations to help detect and prevent fraud.

Review paper check processes

The fraud associated with paper checks is as strong as ever.

Checks deposited

- Use one bank account with serialized deposit tickets for remote office deposits and verify activity daily
- Use endorsements that direct returned items to the account of your choice
- Consider using a bank-operated lockbox to centralize and automate payments that are mailed to your office(s)
- Consider solutions to convert check payments to cost-effective electronic receivables

Checks issued

- Review the controls in place for your check issuance process – from the printing of checks to receipt by the payee
- Maintain check stock in locked custody with limited access—audit regularly and without notice
- Secure items related to check issuance such as facsimile signatures and check reorder forms
- Choose quality paper stock that includes security features
- Audit the checks issued with those presented for payment via Positive Pay, before they clear your account

Review your payment practices at least annually to look for opportunities to minimize risk and streamline your cash flow cycle.

Educate employees

Remind them to be suspicious

- Conduct annual training to help identify unusual requests and suspicious behavior
- Question unusual system behavior
- Safeguard user names and passwords
- Do not use passwords that are easy for others to guess, such as names or birthdays
- Be suspicious of unsolicited e-mails and phone calls

Communicating with TD Bank

- Remember that standard e-mail is unsecure, and should only be used for general inquires
- TD Bank will never ask you to provide your account number, user ID, or password in an e-mail
- Alert TD Bank immediately if you suspect your organization has become a victim of online fraud

Put the power of TD Bank to work for you.

Contact your local Treasury Management Officer or call **1-888-388-0408** to learn more about products we offer to help you protect your business from fraud.