Best Practices to Help Mitigate Fraud

The following checklist offers some suggestions on how you can help protect your computer from virus attacks and minimize internet payment fraud.

Be careful about any payment instructions/ account changes received via email

- ❒ Verify any account changes for an employee (payroll) or vendor (invoice) by reaching out directly to that employee or vendor using existing, previously known contact information
- ❒ If you can't confirm all account changes, then set threshold dollar amounts; be careful of account number changes where large dollar payments will be paid in the coming days or weeks
- ❒ Confirm any payment instructions received via email or fax with the requestor using another communication method, i.e., separate email or phone call
- ❒ Avoid opening email attachments or clicking on internet links in suspicious emails
- ❒ Be suspicious of requests that stress urgency, secrecy or the need to act without further confirmation
- ❒ Be selective about what you install on your computer; malicious programs can automatically be installed on a computer while installing other software

Tighten your ACH and wire controls

- ❒ Utilize ACH and check payment blocks or filters to place appropriate limits on payments
- ❒ Use dual controls for ACH and wire payments, using two separate computers (i.e., one person creates the funds transfer and a second person approves the funds transfer)
- ❒ Implement dual approval of all ACH and wire profiles (i.e.: one person authorizes the creation of the ACH/ wire profile template that contains payment instructions and a second person approves the template)

Be on alert for computer hoaxes and phishing scams

- ❒ The emails and websites phishers use are nearly impossible to distinguish from those of the companies they are impersonating; make sure the URL matches the name of the company and watch for poor grammar or spelling
- ❒ Understand that phishers don't just use email; they have also been known to try to collect information using automated phone messages and faxes, including cell phone text messages, often posing as institutions that you trust

Other best practices

- ❒ Be suspicious of emails, internet pages or telephone calls purporting to be from a financial institution requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information; M&T will never ask for this information
- ❒ Prohibit the use of "shared" usernames and passwords for online banking systems; set a different password for each website that is accessed

What to do if you suffer fraud or suspect fraud

In the event you become a victim of fraud, help protect your financial interests with the following recommendations for immediate actions:

- ❒ Contact M&T Bank at 1-800-724-2240 to request that the following actions, and any others you consider appropriate, be taken to help contain the incident
  - Change online banking passwords
  - Confirm any recent account transactions
  - Close existing account(s) and open new account(s) as appropriate
  - Ensure that no one has requested an address change, title change, or PIN change; ordered new cards or checks; or requested other account documents to be sent to another address
- ❒ Cease all activity from computer systems that may be compromised
- ❒ Contact your security officer or other security advisor to ensure you are following appropriate security guidelines and procedures to help contain the situation

If you suspect fraud, contact your relationship manager or Treasury Management Service at 1-800-724-2240 immediately.

See something. **Suspect** Something. **Say** Something.

M&T Bank