



Payment Fraud and Risk Management

Act Today!

- 1. Protect your computer against viruses and spyware by using anti-virus and anti-spyware software and automatic updates. Scan your computer regularly for viruses and spyware.**
- 2. Please review and action the Fraud Prevention and Risk Reduction Checklist inside.**

Payment Fraud - Are You At Risk?

Fraud attacks using ACH and Wire payments have affected a large number of customers and financial institutions across the country. The attackers are very sophisticated, understand the ACH and Wire payment systems and are targeting customers with large account balances. The significant increase in this type of funds transfer fraud involves the exploitation of valid Internet (online) banking credentials belonging to small and large size businesses.

At M&T Bank, we offer several services to protect your business from payment fraud and reduce your risk of exposure to attacks on your personal account information. Our ACH Debit review, Universal Payment Identification Codes and Secondary Token Authentication are just a few ways M&T Bank protects you and your company's information from being compromised. We require Token Authentication on all Web-based payment initiated services.

How It Can Happen

Often compromise of a customer's account is carried out via a "phishing" E-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Web site. The E-mail recipient is generally a person within a company who can initiate funds transfers or payments on behalf of the business. Once the user opens the attachment, or clicks the link to open the Web site, malware is installed on the user's computer which usually consists of a Trojan keystroke logger ¹, which harvests the user's corporate online banking credentials.

The fraud is carried out when the "fraudster" creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through ACH or Wire that are directed to the bank accounts of willing or unwitting individuals often within a couple days, or even hours.

¹**Keystroke logging** (often called **keylogging**) is the practice of noting (or logging) the keys struck on a [keyboard](#), typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

Your Fraud Prevention and Risk Reduction Checklist

Commercial and small business customers need to operate in secure ways, including Account Controls:

- Utilize payment limitations with ACH and Check payment blocks or filters
- Reconcile banking transactions on a daily basis to identify and review any unknown payments
- Initiate ACH and Wire payments under dual control, with a transaction originator and a separate transaction authorizer (approver), review your payments before sending

Train staff to protect access to personal, financial, and Internet log-on credentials:

- Be suspicious of E-mails and Internet pages 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.
- Avoid opening E-mail file attachments or clicking on Internet links in suspicious E-mails; doing so could expose your system to malicious code that could hijack your computer
- Call your bank and confirm the validity of all requests for personal, financial or account information, particularly if they seem urgent even if they seem routine in nature
- Always sign-off from your Online Banking session. M&T will not ask you to confirm account or log-on details at the end of your session
- Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters and change it regularly (at least a few times each year)
- Prohibit the use of “shared” usernames and passwords for online banking systems. Set a different password for each website that is accessed
- Avoid using automatic “save” login features that remember usernames and passwords in Web browsers for online banking

Assure best practices to secure computer systems and tighten Internet controls:

- Customers that send high value or large numbers of online payments should carry out all online banking activities from a stand-alone, hardened and completely locked down computer
- Install a dedicated, actively managed firewall which limits the potential for unauthorized access to a network and computers
- Use of a secure session (https not http) in the browser for all online banking- M&T supports secure sessions
- Activate a “pop-up” blocker on Internet browsers to prevent intrusions

- You can verify that you are at a secure website by “double-clicking” on the padlock icon located at the bottom of your browser application and reading the site information in the box that appears (it should be a web address that you recognize)
- Regularly update your anti-virus software on your PCs and systems to help protect your information.

In the event you become a victim of fraud, there are a number of immediate recommendations you should take to help protect your financial interests:

- Immediately cease all activity from computer systems that may be compromised
- Unplug the Ethernet or cable modem connections to isolate the system from remote access
- Immediately contact M&T Bank at 1-800-724-2240 so that the following actions may be taken as a priority to contain the incident:
 - Online access to the accounts should be disabled (log-off and re-boot PC)
 - Online Banking passwords changed
 - New account(s) opened as appropriate
 - Ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address

Fraud Prevention Services Available at M&T Bank

M&T Bank has a variety of Fraud Protection services available to you to help protect you from having your companies information compromised.

ACH Monitor Fraud Review helps protect corporate checking accounts from unauthorized ACH debits. For added security, M&T offers two levels of service: block *all* ACH debits from your account or authorize *specific* debits from select vendors.

Universal Payment Identification Code (UPIC) allows you to receive ACH credits without revealing sensitive bank account information. A unique account number and Federal Reserve routing number are assigned so that you do not need to reveal your confidential account number. UPIC account numbers cannot be used to debit your account via ACH transactions or used to access your account.

Payee Positive Pay Payee Positive Pay compares the payee name, dollar amounts, and serial numbers on checks presented for payment to the payee name in a customer-provided check issue file. Variations in payee name, including spelling errors are reported so that customers can then review the suspect check for a pay or return decision.

Check Block can help protect your deposit account from fraudulent or unauthorized check writing activity. This service will automatically return all checks presented against your account, while allowing you to continue to send and receive electronic payments or deposits.

Secondary Approval can help by requiring two users to agree to send ACH, Wire, or Positive Pay Check payment. This service can be set up using the Web InfoPLU\$ Internet site so that one user sends a payment and a second user makes final approval.

Secondary Token Authentication provides you with an additional level of protection against data compromises by giving you a 'unique' number each time you log-on to the internet to send Wire and/or ACH payments. Tokens are required to send ACH and Wire Internet payments at M&T Bank.

For additional information, please contact M&T Bank's Commercial Service Team at 1-800-724-2240.