PAYMENT FRAUD AND RISK MANAGEMENT

HELP PROTECT YOUR COMPANY AND ACCOUNTS FROM PAYMENT FRAUD

M&T Bank

RISE IN PAYMENT FRAUD — ARE YOU AT RISK?

ACH and wire payment fraud is a global and industry-wide issue affecting a large number of customers of financial institutions around the world. The fraud attackers are very sophisticated, understand the ACH and wire payment systems and are targeting customers with both small and large account balances. The significant increase in this type of funds transfer fraud involves the exploitation of valid internet banking credentials belonging to businesses and organizations of all sizes.

HOW IT CAN HAPPEN

Many payment fraud attacks begin with a "phishing" email, which contains either an infected file or a link to an infectious website. The email recipient is generally a person within an organization who can initiate funds transfers or payments on behalf of the organization. Once the email recipient opens the attachment, or clicks the link to open the website, malware is installed on the recipient's computer. This malware usually consists of a Trojan keystroke logger,[1] which harvests the recipient's online banking credentials.

Once the "fraudster" has the recipient's online banking credentials, they can create another user account from the stolen credentials; or directly initiate a funds transfer masquerading as the legitimate user. These transfers have occurred through ACH or wire transfers 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.

BEST PRACTICES TO HELP MITIGATE PAYMENT FRAUD

The following checklist offers some suggestions on how you can help protect your PC from virus attacks and minimize internet payment fraud. This checklist is general in nature and is not geared toward any client's particular situation. Please consult with your security officer or other security advisor to ensure you have comprehensive procedures in place appropriate for your particular organization and needs. It is important that your organization perform periodic reviews of your risks and controls with respect to payment fraud.

TRAIN STAFF TO PROTECT ACCESS TO PERSONAL, FINANCIAL AND INTERNET LOG-ON CREDENTIALS

- ✔ 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
- ✔ Avoid opening email file attachments or clicking on internet links in suspicious emails. Doing so could expose your system to malicious code that could hijack your computer

- Call your bank using a phone number you trust (not one in an email) and confirm the validity of all requests for personal, financial or account information, even if they are routine in nature, but particularly if they seem urgent
- 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 or as may be appropriate for your organization's needs)
- 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" log in features that remember usernames and passwords in web browsers for online banking
- Be selective about what you install on your computer. Malicious programs can automatically be installed on a computer while installing other software

SECURE YOUR COMPUTER SYSTEMS AND TIGHTEN INTERNAL CONTROLS

- Customers that access bank internet sites and/or send online payments should carry out all online banking activities from a stand-alone, hardened and completely locked down computer (e.g. a PC that is not used for email or public Internet browsing)
- Install a dedicated, actively managed firewall, which limits the potential for unauthorized access to a network and computers
- Use a secure session (https not http) in the browser for all online banking
- Activate an appropriate "pop-up" blocker on internet browsers to help prevent intrusions
- Regularly update your anti-virus software on your PCs and systems to help protect your information
- Reconcile banking transactions on a daily basis to identify and review any unknown payments

TIGHTEN YOUR ACH AND WIRE CONTROLS

- Utilize ACH and check payment blocks or filters to place appropriate limits on payments
- ACH and wire payments should be initiated under dual control using two separate computers (e.g. one person creates the funds transfer and a second person approves the funds transfer from a different computer system)
- Implement dual approval of all ACH and wire profiles (e.g. one person authorizes the creation of the ACH/wire profile template that contains payment instructions and a second person approves the template from a different computer system)
- Dual approval of profiles results in all new or modified ACH and wire payment profiles requiring secondary approval prior to being activated

KNOW HOW TO RECOGNIZE COMPUTER HOAXES AND PHISHING SCAMS

- Hoaxes often include a phony warning to "send this to all your friends" and/or incorrect technical language that is intended to frighten or mislead
- Phishers have become very good at impersonating legitimate companies. The emails and websites they use are nearly impossible to distinguish from those of the company they are impersonating
- 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 messages

KNOW HOW TO RECOGNIZE THE SYMPTOMS OF INFECTION

If you experience any of the following, your computer may be infected:

- Your computer is slower than normal
- You are seeing more pop-up boxes than in the past. Many spyware programs track how people respond to these ads, and their presence is a red flag
- Your "homepage" has been changed
- A new toolbar appears at the top or bottom of your screen
- Your computer "crashes." This can even happen when your PC is turned on but you are not actually doing anything

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:

- **Immediately 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 recent account transactions
  - Close existing account and open new account(s), 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
- Immediately cease all activity from computer systems that may be compromised
- Log-off and shut down PC
- Unplug the Ethernet or cable modem connections to isolate the system from remote access
- Immediately contact your security officer or other security advisor to ensure you are following appropriate security guidelines and procedures to help contain the situation

It is important to complete your Payment Fraud and Risk Management Checklist. Commercial accounts are not covered by Federal Reserve Board Regulation E ("Regulation E"). Regulation E applies to individual consumer accounts and provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer (as defined in Regulation E) systems, such as automated teller machine transfers, telephone bill-payment services, point-of-sale (POS) terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The types of accounts with Internet access that are referred to in this document all are commercial accounts and, accordingly, are not covered by Regulation E and its associated consumer rights, liabilities and responsibilities.

SOLUTIONS TO HELP KEEP YOUR PAYMENTS AND ACCOUNTS SAFE

Why be a victim of fraud and be exposed to potential financial losses? At M&T Bank, we offer several fraud services to help you protect your organization from payment fraud and reduce your risk of exposure to attacks on your personal accounts.

PROTECTOR is a security feature designed to mask your log in credentials from key-stroke logging malware to help you protect your Web InfoPLU$® accounts from online payment fraud.

ACH MONITOR FRAUD REVIEW helps protect business 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 only specific debits from select vendors.

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

PAYEE POSITIVE PAY compares the payee name, dollar amounts, and serial numbers on checks presented for payment to similar information in a customer-provided check issue file. Variations in payee name, including spelling errors, as well as variations in dollar amounts or serial numbers, are reported so that you 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 and drafts presented against your account, while allowing you to continue to send and receive electronic payments or deposits.

DUAL APPROVAL can help by requiring two users to initiate and authorize ACH or wire transfers or to confirm decisions to pay suspect checks identified through the positive pay service. Dual Approval can be set up using the Web InfoPLU$® Internet service so that one user sends or accepts a payment and a second user approves the payment.

Dual wire and ACH approval should be established at the company-level on Web InfoPLU$®. As an alternative, clients may continue to manage wire approvals themselves on each wire template they create; however, company-level secondary approval is recommended.

Benefits of company-level dual approval include:

- Convenient, easy-to-implement solution. Clients are not required to update wire and ACH approval controls on each wire and ACH profile (template) they create
- Enhanced fraud protection to help prevent against "account takeover" or "man-in-the-middle" attacks
- Increased peace of mind that all wire and ACH payments will be reviewed and approved by a second user before they are processed

To learn more, contact your local M&T Bank Relationship Manager or M&T Bank's Commercial Service Team at 1-800-724-2240, Monday-Friday, 8am-6pm ET.