Treasury Talk: Top trends and issues

Fraud continues to be one of the biggest challenges businesses face today – ever evolving and growing more sophisticated. To that end, we've devoted this issue to helping you defend against fraud.

In this month's edition:

- Tip of the Month: How to help keep your Treasury Center login credentials safe
- Treasury Center Security Controls
- Protect your accounts with Alerts
- Wire Improvement: ISO 20022 Update

Tip of the Month:

Treasury Center site

-

- Whenever you receive an email that claims to be from M&T Bank or another legitimate business, look carefully at the sender's email address. Does it match who the sender is claiming to be?

We will never send you an email requesting that you click on a hyperlink and enter your login credentials or personal information. If you receive an email that looks suspicious:

- Don't click on the links in the email or open attachments
- Forward details to us at phishing@mtb.com
- Stop all communication with the suspected parties involved

Here are some examples of fake login links.

Be sure to use https://treasurycenter.mtb.com – don't forget to bookmark this URL!

Learn More

Treasury Center Security Controls

Review and customize your users' permissions.

One way to help protect your organization from online fraud is to leverage layered security controls. M&T's Treasury Center's User Maintenance is a key tool in creating layered control by allowing you to restrict user permissions and segregate critical payment functions. Take advantage of customizing permissions with in-depth User Entitlements:

- Add, modify, or delete users as needed
- Use the copy feature to setup a new user with the same rights as an existing user
- Control which accounts each user can view or transact on
- Generate user permission reports to satisfy internal or external audit requests
- Update users' authentication method
- Establish user payment approval limits
- View user audit logs of what each user is doing within Treasury Center

To access the User Maintenance widget in Treasury Center, navigate to:

Want more information? Access the full user guide on User Administration.

Protect your accounts with Alerts

Get notified in real time regarding suspicious activity on your account.

Within M&T's Treasury Center, you can set up helpful alerts to notify you of recent transactions, including any suspicious activity on your accounts (such as new ACH transactions).

The Alert Center is located under the admin menu option.

From the Alert Center, you can add, modify, remove alerts and set -up additional recipients .

Alert Examples:

- Processed/Rejected – Notifies recipient if a payment is received, confirmed, or rejected by the bank
- Suspect Item – Notifies recipient when there are any positive pay/reverse positive pay suspect items that require a decision
- Transaction Notification – Notifies recipient when transactions meet the criteria defined in the alert (i.e. any transactions above or below a defined dollar amount)

For a full listing of Treasury Center Alerts click here.

Learn step-by-step directions on how to set up a transaction alert.

Prefer a tutorial? Watch a 3:24 minute overview video on how to Create an Alert.

ISO 20022 – M&T Bank Wire Update

Creating richer and more structured data across the financial industry.

ISO 20022

Looking Ahead, we are preparing for the Fedwire March 2025 migration to ISO for inbound and outbound messages in line with The Federal Reserve deadline.

Learn More

Contact Us: We’re here to help.

For Treasury Center questions or other Treasury Management services, please contact your Treasury Management Consultant or call M&T’s Treasury Management Service Team at 1-800-724-2240, Monday-Friday, 8am-6pm ET.