WBASNY
WOMEN'S BAR ASSOCIATION of the STATE OF NEW YORK

Presents

Identifying and Protecting Against Common Fraud Tactics

March 30, 2026
6:00 pm - 7:30 pm

Presenters: Leanna Bish
Jodi A. Donato, Esq.
Amy E. Perry

Sponsored by

Nota by M&T Bank

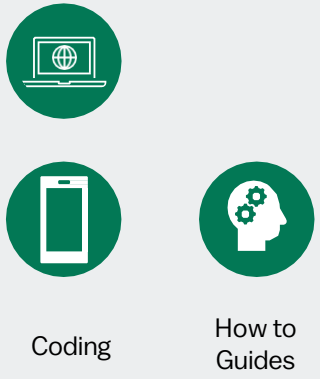
Identifying and Protecting Against Common Fraud Tactics

March 30th, 2026

M&T Bank

2026 Fraud Landscape

Fraud as a Service



The Threat
- Threat Actors have segmented tactics and experience to sell fraud services to a wider net of fraudsters – Lowering the bar for entry
- Enhancements to the speed at which fraud can adjust to market conditions

Risk Mitigators
- Social/Dark Web monitoring

Mail Theft

The Threat
- The source to much of the fraud financing
- Explosive growth since Pandemic and earlier
- Disrupts old logic of "counterfeiting" checks and the technologies deployed to combat it

Risk Mitigators
- Check/ACH Monitoring services

Social Engineering

The Threat
- Primary threat in the fraud ecosystem today
- Targets the human elements of a process to avoid fraud controls
- Shows up in 1000s of variations

Risk Mitigators
- Caution
- Process Speed Bumps

Fraud as a Service

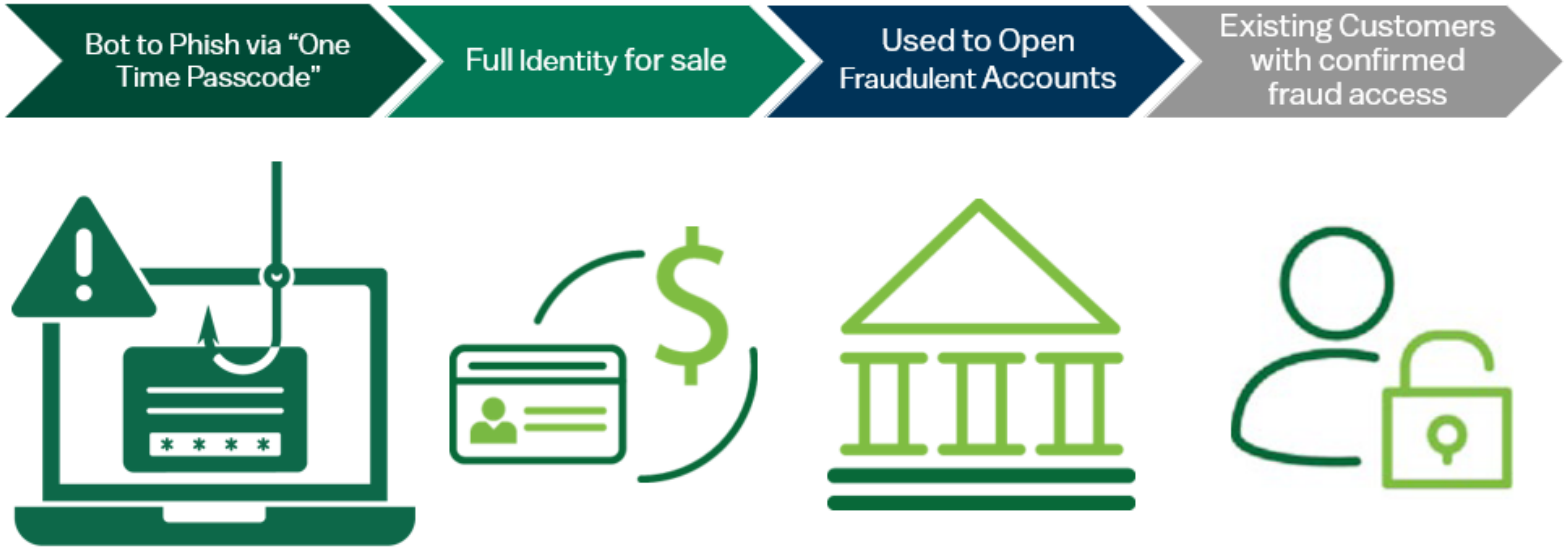
WHAT IS IT?

- Individuals or groups with malicious intent sell tools and services to other criminals, enabling them to carry out various fraudulent activities.

- **Phishing Kits**
  - Pre-made packages simplifying the creation of convincing fake websites, emails, or messages designed to mimic legitimate organizations.
  - These kits allow fraudsters to launch phishing campaigns with minimal technical knowledge or effort.

- **Credit Card Fraud Services/Account Takeover Services**
  - Fraudsters can sell their own services to help others commit fraud.

- Fraudsters also leverage AI and automation to make fraud attacks easier to carry out and more challenging to detect.



All this data is available on the open web with no need for Dark Web knowledge

Who is responsible for all this fraud?

- Fraud Call Centers are big business
  - A growing industry in places like India, Philippines, and Myanmar
  - Many are paid employees of “companies” conducting this activity
  - A growing number are victims of human trafficking/scams themselves

Best Practices for Password Protection

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Passwords should be:

- Longer
- Stronger
- Don’t use info readily available on your social media pages (kid’s or pet names)
- Don’t reuse passwords ESPECIALLY for financial sites
- Don’t share passwords
- Aa3! Use upper case letters, lower case letters, numbers, special characters

Mail Theft

WHAT IS IT?

- The act of stealing mail, particularly checks or other financial documents, with the intent to defraud.
- This can involve stealing checks from mailboxes, intercepting mail in transit, or accessing mail at USPS facilities.

Mailbox fishing

Fraudsters use a sticky substance on a string or other tool to retrieve envelopes from the mailbox, targeting checks, credit cards, and other sensitive information for identity theft and financial fraud.

Stolen Checks

Check washing: Fraudsters will steal checks, often from the mail, and use chemicals (like bleach) to erase the ink, then rewrite the check with a different payee and amount before depositing or cashing it.

8 Details That Can Be Used To Commit Fraud

1. Writer Info – Applied To Counterfeiting Checks
2. Check Number – Gives A Fraudster The Range When Counterfeiting
3. Payee Line – Forged Endorsement Risk; Synthetic Fraud
4. Bank Name – Can Lead To Account Takeover
5. Writer Signature – For Replication
6. Memo Line – Adds Legitimacy When Counterfeiting
7. Routing And Account Number – Aids With ACH Fraud
8. Check Stock – Layout To Be Replicated

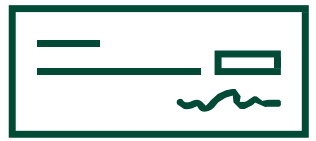
Synthetic Businesses

Karen Corp has an invoice from ABC LLC for $1000 and pays it by check

Fraudster steals the check from the mail

ABC LLC is waiting on payment

Fraudster opens an account for ABC Inc



Fraudster deposits the check in fake account

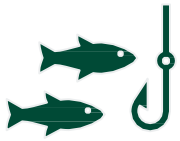
Social Engineering

WHAT IS IT?

- A fraud technique that uses deception and manipulation to trick individuals into giving up confidential information or authorizing fraudulent transactions.
- Targets **people**, not systems

Social Engineering

Fraudster wants to use payment networks to make money



Fraudster uses a phishing message to gather login credentials

Bank controls detect suspicious device and prevents the log on

Fraudster needs a way to not be detected – tries remote access

Using a “tech support” scam to get the customer to call them for repairs

Using remote access tools, the fraudster can utilize the known customer device to initiate login

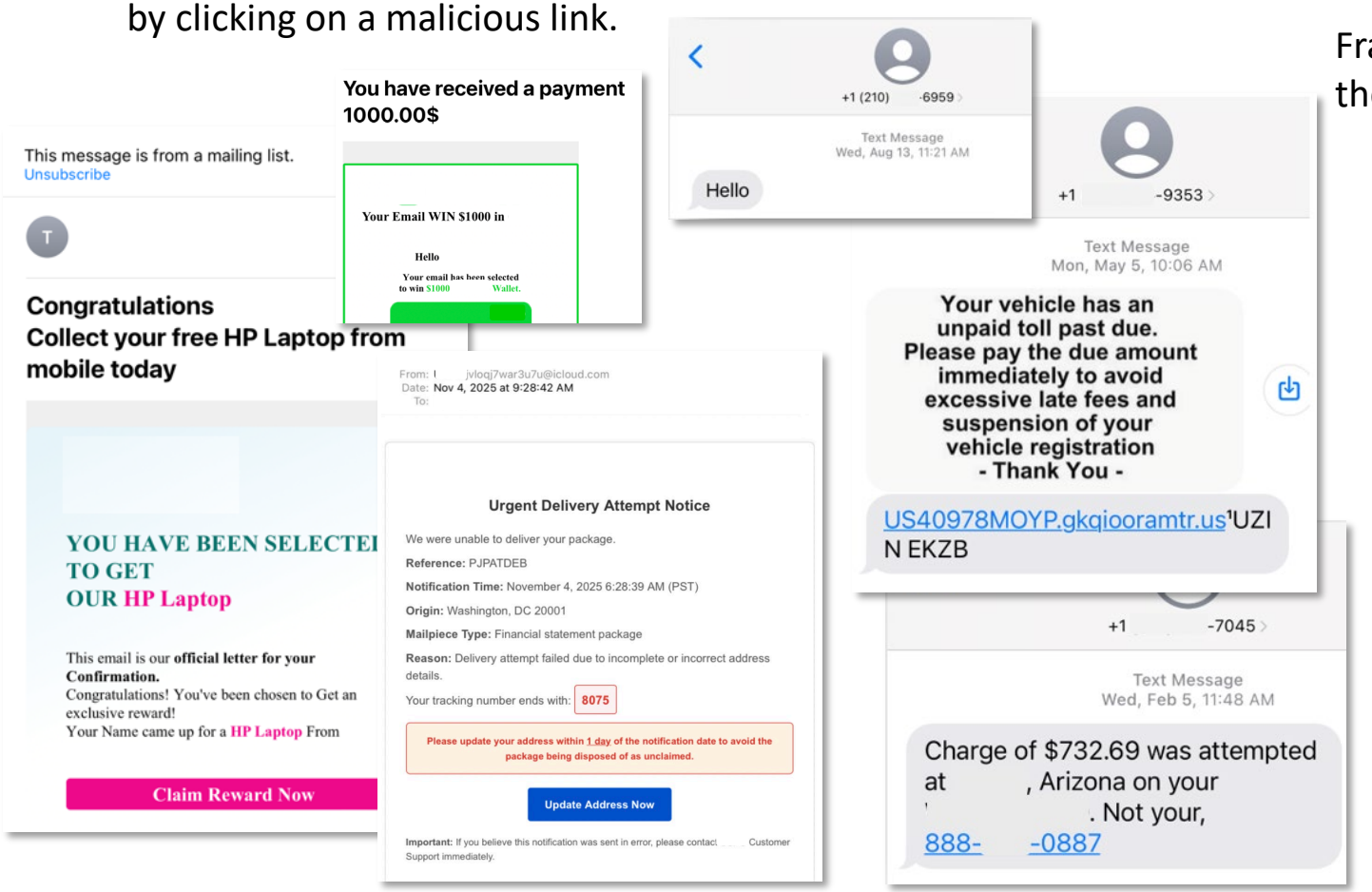
Bank controls detect remote access present on device and prevents login

Fraudster finally calls Contact Center to get bypassed from fraud controls posing as customer.

Social Engineering: Phishing/Vishing

Phishing/Smishing

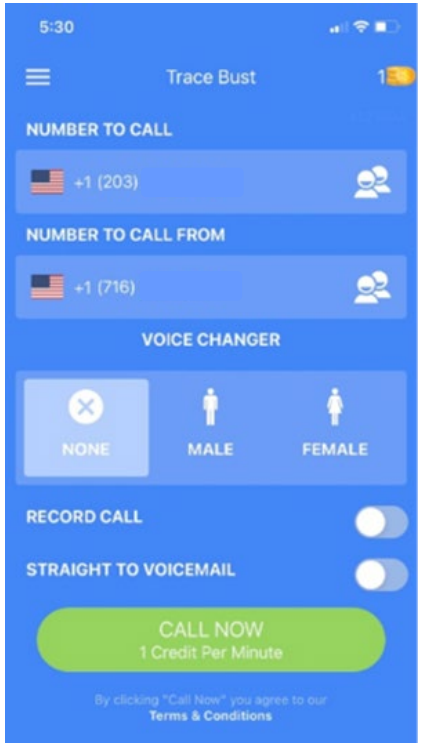
Attackers send fraudulent emails/texts that appear to be from legitimate organizations (like banks or online retailers) requesting users to update their account information, often by clicking on a malicious link.

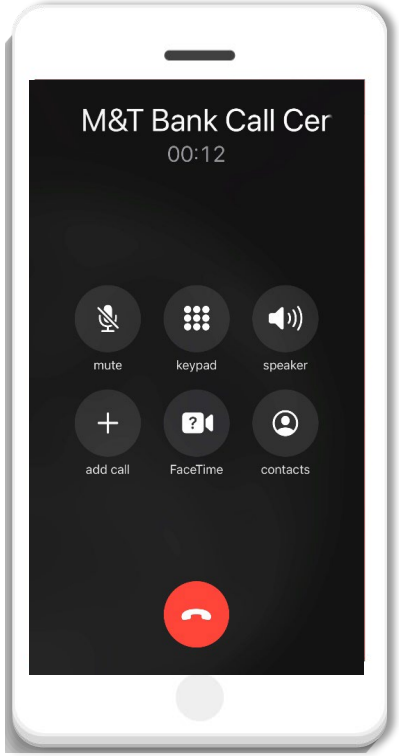


Vishing/Spoofing

Attackers use phone calls to impersonate trusted entities, creating a sense of urgency or fear to pressure victims into revealing sensitive information or making payments.

Fraudsters 'spoof' bank phone numbers to appear as if they're from that organization.





Social Engineering: Business Email Compromise (BEC)

- Large corporations
- Small to midsize businesses
- Retail customers

251 Days

Is the typical time a bad actor is within an environment before impact

Social Engineering: AI Deepfakes & Impersonation

WHAT IS IT?

- Deepfakes are manipulated media – images, videos, or audio which are edited or generated using artificial intelligence tools and may depict real or non-existent people.
- The advancement of technology is making it increasingly harder to spot a deepfake.

<u>How to Spot a Deepfake</u>

- Excessive blurring and inconsistencies around the edges of a face
- Inconsistent skin tone or lighting around the face, as compared with other regions around the face or surrounding conditions
- Poor synching between audio and video
- Speech may be monotonous or unnatural

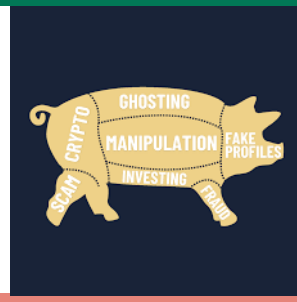
Social Engineering: Account Takeover

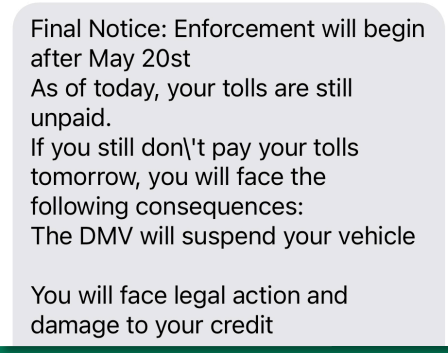
- Fraudsters are calling customers pretending to be employees of banks
  - Using fake names and real employee names found on social media
- Telling customer their account has had recent fraud or their online banking needs a malware update
  - Customer gives access
- Fraudster tells customer to stay out of online platforms while fix is applied
- Fraudster changes phone number and address
- Fraudster sends money via Zelle, Venmo, etc. or sets up Payees within Online Banking

M&T Bank

Social Engineering: Scams

- **Pig Butchering:** Scammers build trust over weeks/months – often starting with a “wrong number” text – then persuades victims to invest in fake crypto or trading platforms. Once victims believe they’re earning profits, the scammer vanishes with the funds.
- **Grandparent Scams:** A scammer pretends to be a grandchild or relative in trouble, urgently asking for money. They often request payment through gift cards or wire transfers to avoid being traced.
- **Romance Scams:** Fake dating profiles are used to form emotional bonds. Once trust is built, scammers exploit the emotional connection to ask for money for fabricated emergencies, travel, or investments.
- **Accidental Deposit Scams:** Scammers send money via apps like Venmo or Zelle using stolen accounts, then ask for it back. If you return it, you’re sending real money – and the original deposit disappears.
- **Computer Software Attacks and Tech Support Scams:** A call, email or pop-up saying your device is infected. The scammer asks for remote access or payment to “fix” the issue, but they’re really stealing data.
- **Delivery Text Scams:** A fake message claims there’s a problem with your package and includes a link. Clicking it leads to a phishing site that steals your personal or payment info.
- **Urgency or threats and requests for secrecy (i.e. IRS/Gov’t Impersonation Scams):** Threats from authority figures can come from people impersonating government agencies or other officials – IRS, Medicare, Social Security, utility co. – who threaten dire consequences for those who won’t pay a made-up fee.





Fraud Education & Awareness Resources

Social Media

Passion or pressure? Spot the red flag.

M&T Bank

If you're caring for an older adult—or just looking out for someone you love—stay alert to these red flags. Romance scams and online fraud often target the elderly and vulnerable, and the emotional toll can be just as devastating as the financial one.

If you're a caregiver or know someone who may be at risk, help them stay safe by watching for these signs:

- Unsolicited friend requests or private messages **OR TEXTs**
- Overuse of the word "trust" early in conversations
- Fast-moving relationships—talk of love or future plans too soon
- Refusal to meet in person, **but may FaceTime or meet over Zoom Calls**
- Requests for money **for new investment opportunities** or tied to emotional stories (medical issues, emergencies, etc.)

Protect their heart—and their wallet.

Learn more about scams targeting vulnerable adults: [link to scam page]

Customer Emails

M&T Bank

Together we can fight fraud.

Protecting seniors and vulnerable adults

Learn More

At M&T Bank, we help you stay one step ahead of fraudsters by exposing their strategies and tactics. This month, we're looking at the many ways they prey on seniors and other vulnerable adults, including:

Imitating a government agency, utility company, or the police and threatening severe consequences unless an immediate payment is made

Claiming someone has won a lottery or received a large inheritance but must first pay substantial taxes and fees to collect their funds

Impersonating a grandchild, asking for money to cover an "emergency expense," then pleading that the victim never tells their mom and dad

Digital Branch Signage

Vulnerable adults

Three common scams targeted to this group:

1. Relationship scams
2. Investment scams

Branch Flyer

Financial Scammers & At-Risk Adults: How to stay safe

Fraudsters prey on everyone—and their increasingly sophisticated and malicious attempts are becoming harder to identify. Criminals target at-risk adults (those with care and support needs) and the elderly, as they are considered more trusting and less tech-savvy, with a tendency to sometimes be confused or disoriented. The 60+ age group lost a record $4.9 billion through fraud in 2024 and submitted 147,000 complaints—more than any other age group and 43% more than in 2023, according to the FBI. This figure is likely even higher, as those who've been defrauded are often too embarrassed to come forward. **To help guard against victimization, know the common types and signs of potential financial abuse.**

Top financial scams that exploit vulnerable adults

A financial abuser can be a stranger, a friend, a caregiver, or even a relative who encourages a vulnerable adult to part with money. While the popularity of personal computers means fraudsters often employ online scams, fraud can also take place on the phone, through the mail, or even show up at the front door.

Urgency, threats, and requests for secrecy

- **Grandparent scams** involve fraudsters call elderly people claiming to be (or be with) a close relative in a crisis situation (accident or arrest). The scammer may ask the grandparent "please don't tell my folks," and then hand the phone to someone posing as a lawyer seeking payment for bail or other costs. With the rise of artificial intelligence (AI), crooks can even clone the voice of a trusted family member to make the scam seem more legitimate.
- **Authority figure threats** can come from people impersonating government agencies or other officials—e.g., the IRS, Medicare, Social Security, or utilities—who threaten dire consequences for those who won't pay a made-up fee.

Suspicious solicitations

- Bad actors may make requests for funds or financial data in the guise of a great money-making investment, a sympathetic ploy for a charitable donation, or another scheme.
- Support staff remote access online solicitations occur when an email or pop-up message says there is a virus or some other frightening claim that requires calling a certain number, leading to a fraudster. The scammer then convinces the individual to provide remote access to the device in order to "rectify" the situation, but instead gains access to a device or computer.

Computer software attacks

- Bad actors may send malicious software (malware) links in emails or pop-ups. Trusting adults click on the carefully embedded links that are designed to take over computers, providing access to bank or other financial account details.

Too-good-to-be-true offers

- Windfall scams send news of a lottery jackpot, inheritance, or other prize winnings—but say a certain amount needs to be wired to cover taxes or other costs before money can be claimed.
- Sweetheart hoaxes involve fraudsters posting on social media or creating fake dating site profiles,

M&T Bank

Best Practices

Best Practices: What You Can Control

Protect Yourself

- See Something, Say Something
- Ignore Unsolicited Emails
- Use Email Services That Incorporate Phishing Defenses
- Be Aware Of The Latest Scams
- Protect Your “Digital Identity”

Protect Your Access

- Use multi-factor Authentication
- Use Complex Passwords: DO NOT SHARE
- Change Passwords Regularly
- Use A Password Keeper/ Generator App
- Use Unique Passwords
- Avoid Google searches for bank website

Protect Your Business

- Investigate Employees & Vendors
- Update For Terminations
- Always Confirm Instructions Verbally
- Segregate Duties
- Work With Vendors To Be Sure They Are Secure
- Make Cybersecurity A Regular Conversation
- Create Security Awareness Training For All Employees

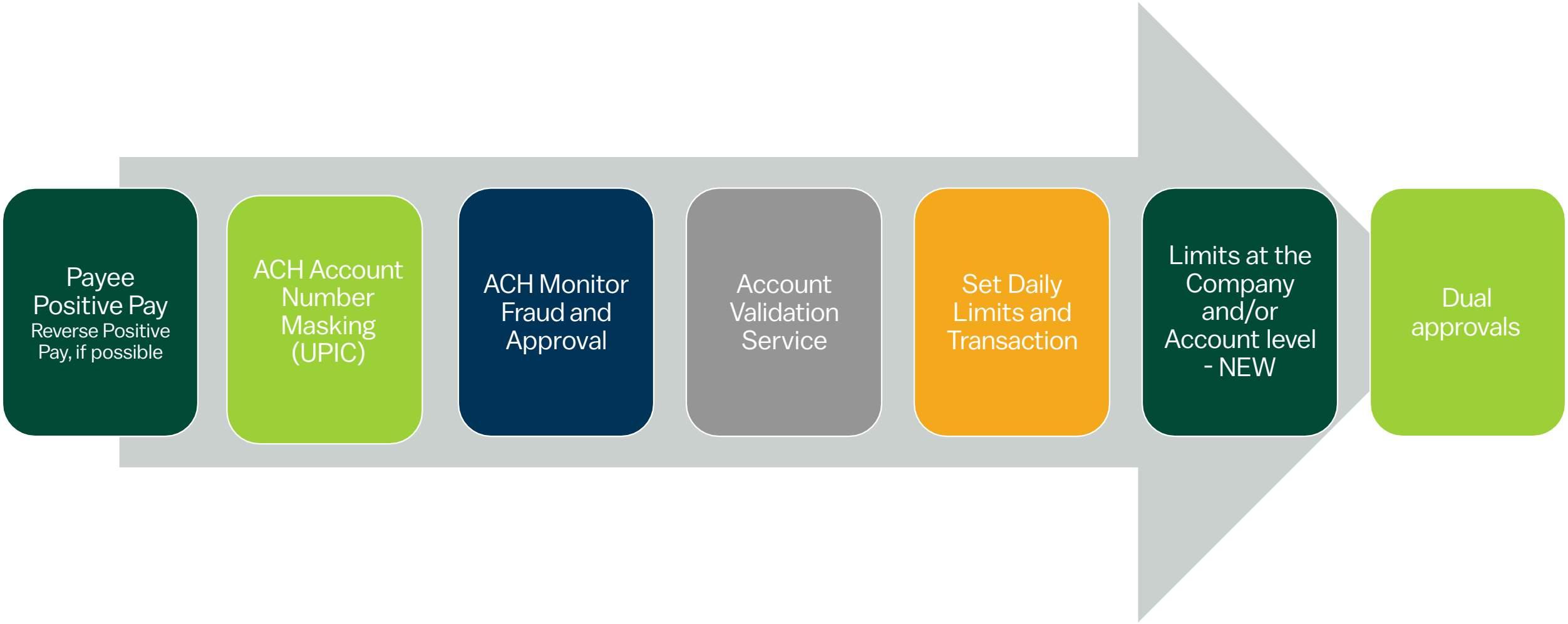
Protect Your Technology

- Use Anti-virus & Anti-spam Software
- Use Dedicated Computers
- Log Off Computers
- Install Software Updates Promptly To Patch Vulnerabilities
- Keep A Consistent Schedule For Backups
- Use Anti-virus Software For All Devices Including Phones

Protect Your Payments

- Safeguard Check Stock
- Audit Randomly
- Reconcile Accounts Daily
- Establish Dual Approval
- Explore Fraud Protection Services On Bank Accounts
- Explore Cyber/ Fraud Insurance
- Establish Payment Procedures & Follow Them
- Dual Administration
- Review Transactions Regularly
- Support Callbacks

Best Practices: What M&T Offers



What should I do if attacked by fraud?

Time is critical.

The sooner you can notify the bank, the sooner we can try and retrieve funds

01

Notify your bank

They can help expedite a resolution

02

Change all passwords

Don't reuse old passwords

03

Review past payments

Get a top-line view of all transactions

04

Stop unprocessed / questionable payments

Real-Time payments will not be able to be cancelled

05

File Police Report

Aids in investigation and potential insurance claims

Disclosures

- This presentation is for informational and educational purposes only. Nothing herein should be considered or relied upon as legal advice. The author assumes no responsibility or liability for the specific applicability of the information provided. Please consult your own legal counsel for any legal advice.

- Some products and services referenced herein may be provided through subsidiaries or affiliates of M&T Bank.

- Unless otherwise specified, all advertised offers and terms and conditions of accounts and services are subject to additional terms and conditions and change at any time without notice. All products and services are subject to eligibility and restrictions may apply. After an account is opened or service begins, it is subject to its features, conditions and terms, which are subject to change at any time in accordance with applicable laws and agreements. Please contact an M&T representative for full details.

Thank you

This presentation is for informational purposes only and does not constitute legal or other professional advice. As such, this information should not be used as a substitute for consultation with professional data security, legal or other advisers. M&T Bank does not provide legal advice and, accordingly, nothing presented herein should be deemed or construed to be legal advice provided by M&T Bank. If professional advice is needed, the services of a professional advisor should be sought.

All M&T Treasury Management services are subject to M&T's standard Treasury Management Services Agreement and Treasury Management Services Product Terms and Conditions for that service. All products and services are subject to eligibility and restrictions may apply.