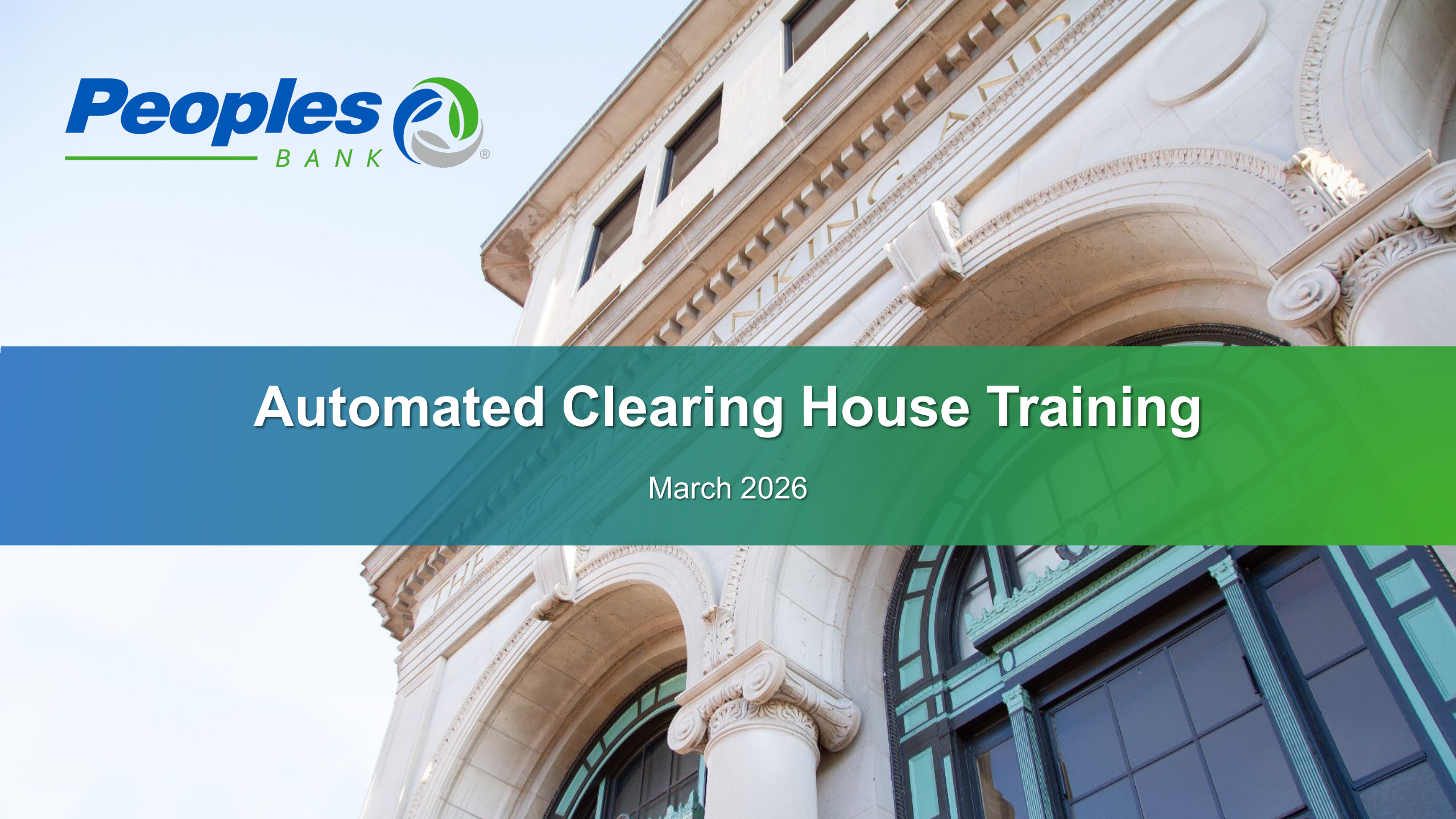


Automated Clearing House Training

March 2026

Table of Contents

- Automated Clearing House (ACH)
- ACH Network
- Standard Entry Class Codes (SEC)
- ACH Services Offered
- As an Originator
  - Agreements
  - Authorizations
  - Proof of Authorizations
  - Recurring Transactions
  - Prenotifications
  - Same Day
  - Returns & NOCs
  - Health Care
  - Third Party
- Annual ACH Reviews
- Rule Changes
- NACHA Rule Violations
- Fraud
- Fraud Prevention
- Security Actions

This annual ACH training is intended for anyone processing or approving ACH transactions via online banking.

Peoples BANK

Automated Clearing House (ACH)

ACH

Electronic payments or credits are completed in standardized formats that allow these banking transactions to be sent anywhere in the United States.

NACHA

The National Automated Clearing House Association (NACHA) – The trade association for the electronic payment associations, which establishes the rules, industry standards, and procedures governing the exchange of commercial ACH Payments by depository financial institutions.

ACH Network

Funds transfer system governed by NACHA rules, which provides the clearing of electronic entries for participating financial institutions.

Virtually every major bank is affiliated with NACHA or works with a local clearinghouse.

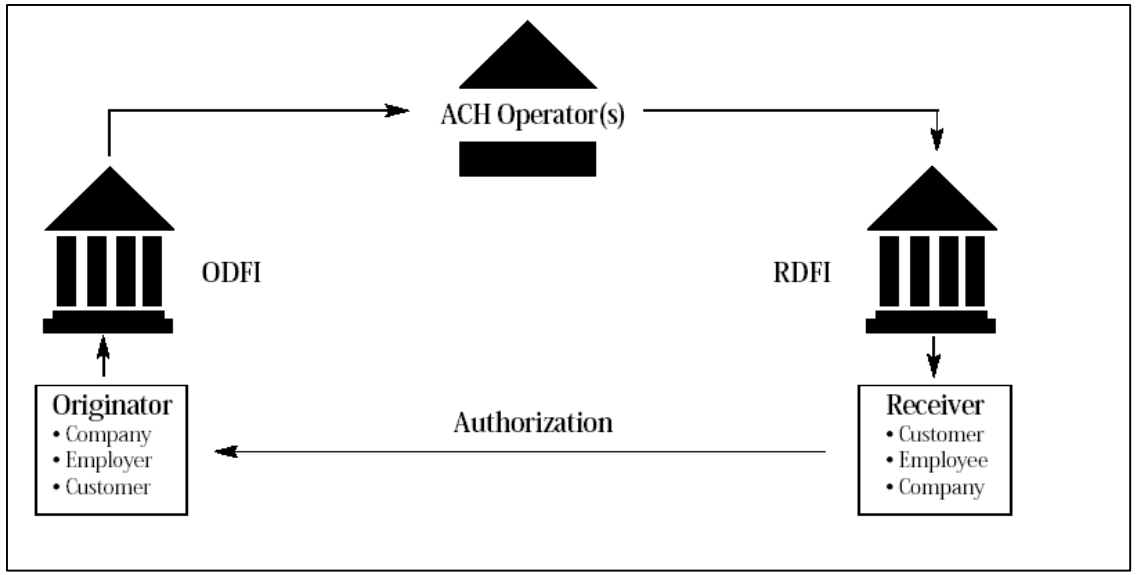
***NACHA manages the development, administration, and governance of the ACH Network, the backbone for the electronic movement of money and data.**

Peoples BANK

ACH Network

Five Participants in ACH Process:

1. Originator company or individual
2. ODFI (Originating Depository Financial Institution)
3. ACH Operator (FED)
4. RDFI (Receiving Depository Financial Institution)
5. Receiver



Standard Entry Class (SEC) Codes

PPD (Prearranged Payment and Deposit)	• *Prearranged payment and deposits*. Used to credit or debit a consumer account. • Used for Payroll, Pensions, etc. • Allows for one Addenda Record. • Written authorization is required for debits and highly recommended for credits.
CCD (Cash Concentration or Disbursement)	• *Corporate credit or debit*. Primarily used for business-to-business transactions. • An agreement must be in place between the originator and receiver. • Can contain addenda records; when included, this format may be referred to as CCD plus.
CTX (Corporate Trade Exchange)	• Designed for companies with trading partnerships or used when sending payments to the government (example, child support payments). • Allows for 9,999 addenda records per ACH payment. • Child Support payments are either CCD+ or CTX.
RCK (Re-Presentation Check Entry)	• Format is used to represent a returned check through the generation of a single-entry ACH debit. The RCK SEC allows for a single-entry ACH debit transaction to re-present a paper check after the paper check has been returned for either insufficient or uncollected funds. • Amount up to and including $2,500. • Be dated less than 180 days from the date the entry is transmitted to the RDFI.
Addenda Records	• Optional and supply additional information about the Entry Detail Records or payment-related details. • The addenda record detail is machine-readable (EDI-Electronic Data Interchange). Each addenda record can be up to 80 characters. If the addenda record exceeds 80 characters, then the data will wrap to the next addenda record. This allows for 800,000 bytes of data for each ACH payment in the CTX format.

Peoples BANK

ACH Services Offered by Peoples Bank

ACH transactions are completed using Business Online Banking.

ACH Modules & SEC Code options:

- Payroll (PPD)
- Payments (PPD/CCD/WEB)
- Collections (PPD/CCD/WEB)
- Uploads (PPD/CCD/WEB)
- Tax Payments (CCD)
- Same Day ACH (PPD/CCD)

ACH Transaction completed thru online banking may include:

- Direct Deposit of Payroll
- HSA payments
- Collecting utility payments
- Business-to-Business Payments
- Federal Tax Withholdings

All ACH Files must be drafted and approved no later than 5:00 pm Eastern Standard Time (EST).

Daily 5:00 pm EST cutoff is required for files to be sent to the Federal Reserve.

Peoples BANK

As an Originator: Agreements

Each originating company must have a signed ACH agreement on file with Peoples Bank.

- This agreement defines the parameters between the parties
- Establishes liabilities
- Binds the Originator to the NACHA Operating Rules
- Binds the Originator to applicable U.S. Laws

If you submit an incorrect or invalid ACH file and it needs to be reversed, there will be a $100.00 ACH Reversal Fee imposed. Reversals need to be submitted within 5 banking days of settlement.

ACH Rule Books are available for purchase by visiting
www.nacha.org/store

***Submitted reversals are not a guarantee that Peoples Bank will receive OR recover the funds from the other Financial Institution.**

Peoples BANK

As an Originator: Authorizations

Originators must obtain authorizations from all Consumer Receivers

- Obtain receiver routing number, account number, and type of account.
- Dated and signed or similarly authenticated.
- Credit entries may be authorized orally or in other non-written means.
- Debit entries must be authorized in writing or similarly authenticated.

Originators must have an agreement with all Corporate Receivers

- Agreements vary depending on the complexity of the application.
- Obtain receiver routing number, account number, and type of account.
- Corporate ACH Originators must apply credit to a customer's account effective for the same day he/she receives credit for the transaction.

Each company should have an agreement in place with receivers and/or vendors that defines the parameters between the parties and includes the ability to allow correcting entries if needed.

Peoples BANK

As an Originator: Proof of Authorization

NACHA Rule

If requested, the Originator's financial institution may be required to provide proof of authorization. The financial institution must provide the required information within 10 business days of receiving written request.

What This Means to You?

If requested, you will need to provide the requested information to the bank. If you do not provide the requested information, the return may be posted to your account.

As an Originator: Recurring Debits

If you initiate recurring debit entries:

- If the debit amount varies, you must notify the consumer within 10 calendar days of the change.
- If the debit date varies, you must notify the consumer within 7 calendar days of the change.

ACH data should only be used for the original purposes intended.

- You should have proper authorization to debit, credit, etc.

Peoples BANK

As an Originator: Prenotifications

Prenotifications (also known as Prenotes)

- Zero-dollar entries submitted to verify the receiver's account information at the RDFI.
  - Optional, but highly recommended.
- A return or notice of correction may be issued if account information is invalid.
- Per NACHA, if a prenote has been initiated, a live dollar entry should not be submitted for 3 banking days after the prenote was issued.

Peoples BANK

As an Originator: Same Day

Same Day ACH - This simply means some payments can process quicker, virtually the same business day.

- Originators need to be enrolled in Same Day processing to originate Same Day ACH transactions.

- All Same Day ACH Files must be drafted and approved no later than 2:00 pm EST.
  - If a file is submitted after the cut-off, it may not be processed as a same-day file.
  - The receiving bank has until 5:00 pm EST to post Same Day transactions.

- Pricing is higher than next-day ACH transactions.
  - Please speak with your Treasury Management Officer for pricing information.

Peoples BANK

As an Originator: Returns and Notifications of Change

- **Notices & Alerts:**
  - The online banking system will generate an alert/notice to the employees with ACH Reporting enabled.
  - To view the ACH Reports, click ACH Reports within online banking daily to monitor NOCs and Returns.
  - Once the notice is received, the account information should be updated prior to initiating any future ACH transactions.
  - It is your responsibility to correct all incorrect information.
  - If you need assistance, please reach out to Business Support at 800.374.6123, opt 6, or your Treasury Management Officer.
- If you do not make the necessary changes and we continue to contact you regarding the same NOC repeatedly, you could be subject to fines or termination of ACH services by NACHA and/or Peoples Bank.

- **Items returned for Unauthorized Consumer Entries**
  - May be returned to the Originator within 60 days from the settlement date.

- **Items returned for Unauthorized Corporate Entries**
  - Must be returned to the Originator within 24 hours of the settlement date.
  - Keep in mind that as a business, you only have 24 hours to dispute an unauthorized debit to your business account.

Peoples BANK

As an Originator: Returns and Notifications of Change

Returns

- **Reasons items may be returned:**
  - Closed Account (R02)
  - Insufficient Funds (R01)
  - Stop Payment (R08)
  - No account/Unable to locate account (R03)
  - Unauthorized (R05)

Notifications of Change (NOC)

- **Reasons for Notifications of Change**
  - Incorrect Account Number (C01)
  - Incorrect Transaction Code (C05)
  - Incorrect Routing Number (C02)

It is your responsibility to make corrections within 6 banking days. If you do not make the necessary changes and we continue to contact you regarding the same NOC repeatedly, you could be subject to fines or termination of ACH services by NACHA and/or Peoples Bank.

ACH Rule Books are available for purchase by visiting
https://www.nacha.org/store

Peoples BANK

As a Health Care Originator:

If you are originating health care EFT's you should include:

- HCCLAIMPMT in the Company Entry Description Field of the Company/Batch Header Record for Health Care-related Payments.
- Company Name Field in the Company/Batch Header Record so it can be recognized by the receiver.
- Populate the Payment Related Field of the Addenda Record with the appropriate data segments.
- Make sure you follow the formatting characters in the Payment Related Field of the Addenda Record.

Peoples BANK

As a Third-Party Originator:

Third Party pertains to companies originating ACH transactions on behalf of another party.

- **A Separate online banking agreement may be required to conduct these transactions.**

- **Addendum Requirements:**
  - The name of the originating company must be provided for all ACH transactions.
  - Type of ACH transaction being completed.

- **Annual ACH audit required for transactions**
  - As a third-party originator, you could be asked to provide your annual audit results.
  - This is an audit your company completes, and you may be asked by the financial institution to provide a copy of the completed audit.
    - These results should include record retention, data security and other related items.

- **Third Party Sender (TPS) Registration, effective since September 2017, requires financial institutions to register Third Party Sender relationships with NACHA.**
  - TPS should be aware that their financial institution may request information from them regarding the clients they are processing ACH files on behalf.

Peoples BANK

Annual ACH Reviews

Regulators require ACH limits and relationships to be reviewed annually.

- You may be required to provide financial data yearly to maintain your ACH access and limit.
- This includes Financial Statements and/or Tax Returns.
- We may require originators to process ACH transaction using prefunding. This means sufficient funds must be available in the originator's account at the time of ACH file submission, as the funds will be debited at the time the file is processed.

For your business's security:

- If you do not use the ACH services for 180 consecutive days, we may disable your access, and you may be required to start the approval process over.

Peoples BANK

Rule Change

Preparing for Updated ACH Payment Description Requirements. Starting **March 20, 2026**, ACH rules will establish a new standard description for specific content within the "Company Entry Description" field.

To maintain compliance, please note:

- PPD credits for wages/salaries should include the term "payroll."
- WEB debits for e-commerce/online retail purchases should include the term "purchase."

*We recommend reviewing and updating your payment systems in advance of this deadline.

Click below for additional information on the rule change

NACHA Rule Changes

Peoples BANK

NACHA Rule Violations

3 Classes of Rules Violations

- **Class 1 Violation fines**
  - First recurrence – Up to $1,000.00
  - Second recurrence – Up to $2,500.00
  - Third recurrence – Up to $5,000.00
- **Class 2 Violation fines**
  - Up to $100,000.00 per month until the issue is resolved.
- **Class 3 Violation fines**
  - Up to $500,000.00 per month until the issue is resolved.

ACH Rule Books are available for purchase by visiting https://www.nacha.org/store

Impact of Rules Violation

- If you continue to disregard a Rules Violation, your ACH privileges may be suspended and/or your company could be banned from utilizing the ACH network.

National System of Fines | NACHA

- **Visit NACHA.ORG for a complete listing.**

Peoples BANK

Fraud

All It Takes is One Click – Don't Be a Victim

- Your security matters to us. The best defense against fraud is awareness – learn how to recognize common scams and safeguard your information, technology and finances.

If you suspect fraudulent activity on your Peoples Bank account, call 800.374.6123.

- To keep up to date, please visit our **Fraud Center**.

For more information on types of fraud, visit
FTC - Cybersecurity Basics

Peoples BANK

Fraud - Types of Cyberattacks

Spoofing

A scammer disguises their identity to look like a trusted source, such as your bank or a known company, to trick you into sharing personal information or sending money.

How to Spot It:

- The message feels urgent or threatening.
- The caller or email asks for personal or account information.
- The phone number or email address looks slightly off.

What To Do:

- Hang up or delete the message and contact the company directly using a known phone number or secure website.

Phishing

Fraudsters send fake emails, texts or messages that look real to get you to click on a link, share your login details, passwords or account numbers.

How to Spot It:

- Spelling errors or odd phrasing.
- Links that don't match the company's real website.
- Requests for personal information, passwords or payment details.

What To Do:

- Never click unexpected links. You can hover over links to check if the URL matches the legitimate website.
- Verify the legitimacy of the sender by contacting them directly using a known phone number or other known and trusted communication channel.
- Use reliable anti-virus software, keep systems updated and regularly back up files offline.

Peoples BANK

Fraud - Types of Cyberattacks

Social Engineering

Someone manipulates or pressures you into giving away confidential information or access – often by pretending to help, creating urgency or playing on emotions like fear or trust.

How to Spot It:

- The person pressures you to act fast.
- They ask for sensitive information or verification codes.

What To Do:

- Verify the request by contacting the person or organization through a separate, trusted communication method.

Business Email Compromise (BEC)

Scammers may impersonate businesses or individuals and send an email urgently requesting payment via wire transfer.

How to Spot It:

- The requester changes payment instructions, such as bank account numbers, wire instructions or payment methods that are not normal procedure.
- The email address has a typo or uses a different domain.
- The requester asks to skip approval, ignore standard vendor verification or use odd payment methods (gift cards, crypto, prepaid cards).
- You get send files or links that weren't requested.

What To Do:

- Don't act – verify the legitimacy of payment requests through a separate and trusted communication method.
- Notify your IT/security team using company procedures.
- If the request is fraudulent, contact your financial institution to recall the transfer and request a Hold Harmless Letter or Letter of Indemnity.

Peoples BANK

Fraud - Types of Scams

Types of Scams	What To Do:
Check Fraud: Altering a legitimate check for a different amount or an unauthorized recipient.	Consumers can use Direct Deposit and Bill Pay, while businesses can use Remote Deposit Capture and Positive Pay.
Romance Scams: Fraudsters create a fake online profile (dating apps and social media) with the goal of gaining your trust to steal money or personal information.	Don't trust anyone you haven't met in person who asks for money, do not share personal/ financial information and do not send them money.
SIM Swapping: Your phone number is transferred to a different SIM card under the control of a criminal who is then able to intercept texts/calls, including security codes to access your accounts.	Add SIM Protection to your phone plan and use strong/unique passwords for your accounts. Don't share verification codes, PINs or passwords with anyone – even if they claim to be from your phone company or bank.
Payment Scams: Tricks to get you to send money (gift cards, wire transfers or crypto) to a scammer through fake invoices or urgent "refund" requests.	Never send money or share payment information with someone you don't know or can't verify. Verify the legitimacy of payment requests through a separate and trusted communication method.
Online Shopping Scams: Fake websites and emails posing as retailers or that list items at low prices to steal payment information without delivering products.	Use reputable sites, avoid unfamiliar links or pop-ups and check reviews before buying. Use secure payment methods like credit cards or trusted third-party services, such as Zelle®.[1]

[1]Zelle and the Zelle related marks are wholly owned by Early Warning Services, LLC and are used herein under license. Zelle® requires users to be 18 years of age to enroll and use.

Peoples BANK

Fraud - Types of Scams

Types of Scams	What To Do:
Mortgage Phishing Attempts: Urgent messages about mortgage issues, often appearing to be from their lender.	Ignore and discard messages. Contact your lender directly to verify legitimacy.
Disaster Fraud: Scammers pose as the government or charities to exploit your information and finances under the guise of disaster assistance.	Government employees don't request money for disaster aid. If approached, verify their identity by contacting government agencies or local law enforcement.
Threat of Harm: Scammers may threaten harm to you or family if you don't send money, sometimes using technology to mimic a loved one's voice to convince you.	Use a "safe word" that only you and your family members know to validate the scenario. Report the incident to your bank and contact law enforcement if you feel threatened.
Investment Fraud: You may be contacted with "get-rich-quick" investment opportunities, only to disappear once you invest.	Verify investment offers carefully. Be cautious with requests for personal or financial information, especially for payments via digital currency or instant transfers.
Sweepstakes, Prizes and Lotteries: You may receive notice you won a sweepstakes, prize or lottery and need to provide personal information to "process" your winnings.	If it sounds too good to be true, it likely is. If you didn't enter a contest or are unsure, don't share information. End the communication and contact the organization directly to confirm.

Peoples BANK

Fraud Prevention Daily Tasks and Tips (Online Banking)

Transactions

- Review all transactions for your company. This includes funds transfers, bill payments and ACH files.
- It is a good idea to monitor your accounts throughout the day to manage cash flow.
- Be cautious of unusual requests for ACH payments, especially if they come from unknown parties. Fraudsters may impersonate a known contact or vendor.

User Security

- Delete users who are no longer with the company or no longer need online access.
- Peoples Bank **highly recommends** dual control for ACH & Wire originated transactions.
- Use strong, unique passwords for your online accounts to prevent unauthorized access.
- Never share your login credentials. Each online banking user should have a unique login & password.
- Never share Secure Access Codes (SAC).
- Be cautious of emails or text messages that request your bank account information or payment via ACH transfer.
- Use caution with emails or text messages that have links attached from unknown sources or unexpected messages.
- Maintain secure systems, automate updates if possible.

Additional Information

- We may contact you or someone at your company to confirm file/s are valid and should be processed.
- Educate yourself and your employees on fraud and what to look for. Learn about the latest fraud schemes and tactics used by scammers, such as fake invoicing, vendor impersonation, and account takeovers.
- Monitor computers & networks for unauthorized access.

For more information, visit
Talking Cybersecurity with Your Employees

Peoples BANK

Fraud Prevention Daily Tasks and Tips (ACH)

Each originator needs to evaluate its current policies, procedures and systems to ensure the company identifies safeguards for protected information - non-public information, including financial information of customers.

- Security policies, procedures and systems must:
  - Protect confidential information
  - Protect against threats or hazards
  - Protect against unauthorized use of protected information
- Originators should be willing and able to prove compliance to the financial institution.

Take Action!

Download NACHA Fraud Booklet
Visit nacha.org

Keep up to date with current industry fraud trends and threats. View these additional resources:

- nacha.org
- NACHA Fraud Booklet
- EPCOR Corporate User
- FTC – Protecting Small Businesses

Speak to a Treasury Management Officer regarding our Positive Pay Fraud Prevention Services to help protect your accounts.

If we offered you a commercially reasonable security procedure that you reject, you agree that you are responsible for any payment order, whether authorized or not, that we accept in compliance with an alternative security procedure that you have selected. The Positive Pay service can help detect and prevent fraud and is appropriate for account holders who issue a high volume of checks, a lot of checks to the general public, or checks for large dollar amounts.

Peoples Bank **highly recommends** dual control for ACH & Wire originated transactions.

Peoples BANK

Security Actions

Positive Pay is an effective tool designed to provide protection against check and ACH fraud.

- Positive Pay is a powerful deterrent to ACH and check fraud. We will compare your company's records for issued ACH and check payments (transmitted/uploaded file) with the ACH and checks that are presented for payment. If the pieces of information don't match, then an alert will be emailed, and you can decide to pay or return the item.

- To find out more about this service, please contact your Treasury Management Officer.

Peoples BANK

Security Actions

Secure Access Codes are used as an additional security feature to authenticate and verify the legitimacy of an attempt to access online banking.

Multi Factor Authentication (MFA) is an additional regulation that has been mandated by the FFIEC. Peoples Bank is using Secure Access Codes to comply to this regulation. If your business becomes a victim of fraud or data breach, what should you do?

- Contact your local branch or Business Support at 800.374.6123, opt 6 as soon as you find the breach or notice the fraudulent activity.
- You only have a limited amount of time to recover lost funds. Once the funds have been released from Peoples Bank, we may not be able to retrieve them.
- Discuss Positive Pay Fraud Protection Service with your Treasury Management Officer.
- Peoples Bank offers Fraud Protection Insurance through the Peoples Bank Insurance division. To find out more about this program, please contact them at 800.283.3823.

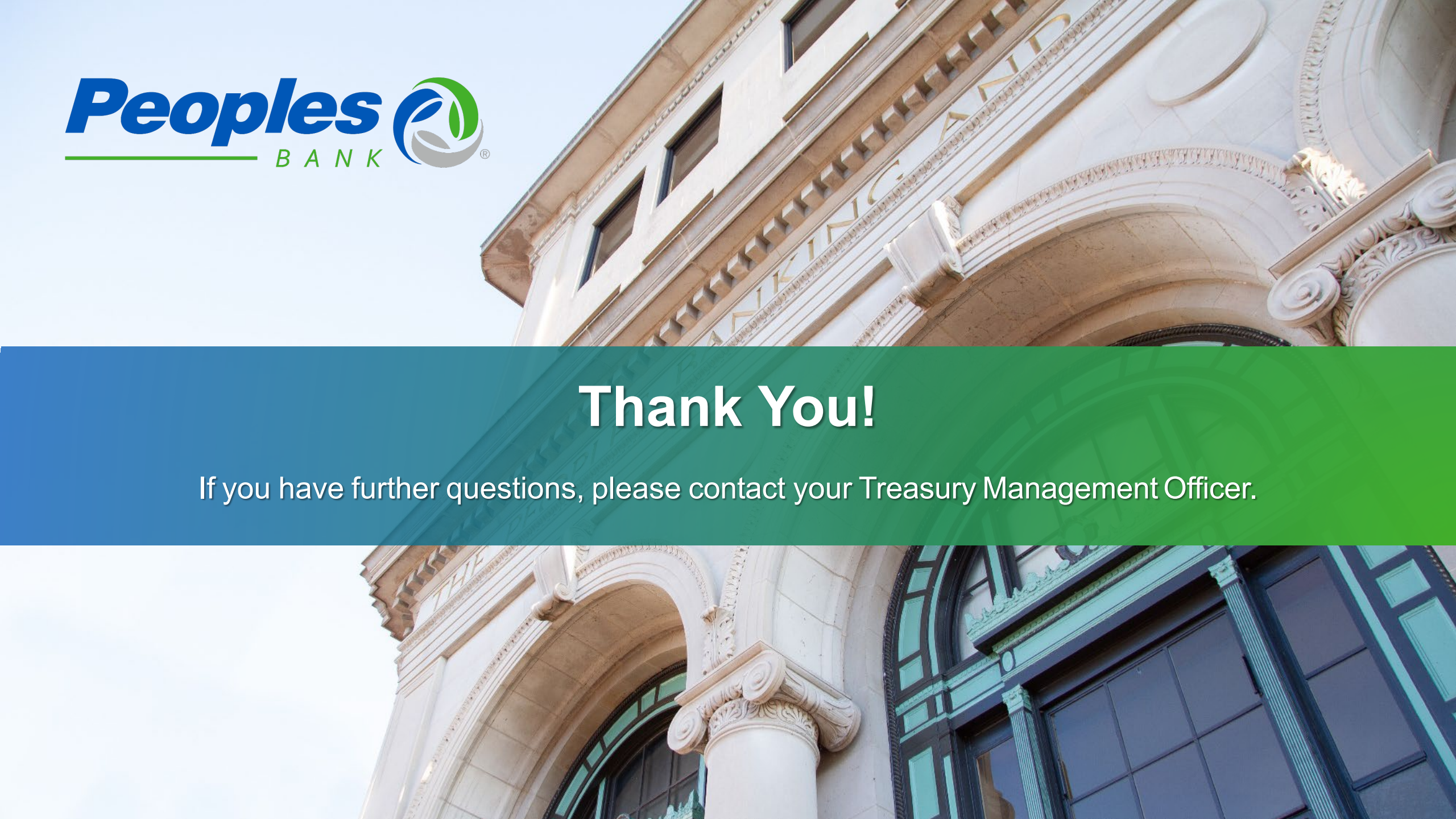
Peoples Bank will **never** call, text, or email you to request your security codes, online banking credentials, debit/credit card numbers, or to complete transactions. We will also never ask to be added as a user on your account or request remote access to your personal or business computer.

Bank impersonators are skilled at getting you to believe your money is at risk. Scammers can make caller ID, emails and texts display as messages from your bank.

If you're ever unsure**, contact your local branch or 800.374.6123 opt 6.** To keep up to date with fraud tactics and scams, please visit our Fraud Center.

Please review: Protect Your Organization From Current Fraud Threats | NACHA

Peoples BANK



Thank You!

If you have further questions, please contact your Treasury Management Officer.