2026 NACHA Rule Updates & Fraud Monitoring Recommendations

March 25, 2026

HARBOR

Dedham Savings

HARBOR

Today's Topics

- 2026 NACHA Operating Rule Changes
- Fraud Awareness
- Fraud Monitoring Recommendations
- Employee Training Recommendations to prevent Phishing
- Operational Tools to Reduce Fraud Risk
- Threat Response Report in Digital One Business

Dedham Savings

Meet the Presenters

Ed Skou

Director of Treasury Management, Dedham Savings

Rolin "Bud" Peets CISSP | CIPM

Chief Protection Architect, Harbor IT

John D. Flory III

Security Practice Lead, Harbor IT

2026 NACHA Operating Rule Changes

HARBOR

Fraud Monitoring by Originators, TPSPs, & ODFIs

Risk-Based Monitoring Requirements

Originators, Third-Party Service Providers (TPSPs), and ODFIs must implement risk-based processes to detect unauthorized entries.

Annual Review: These processes must be reviewed each year to align with emerging risks.

RDFI ACH Credit Monitoring

Monitoring Procedures: RDFIs are required to adopt procedures that identify unauthorized ACH credit entries.

Annual Review: Procedures must be updated annually to ensure ongoing effectiveness.

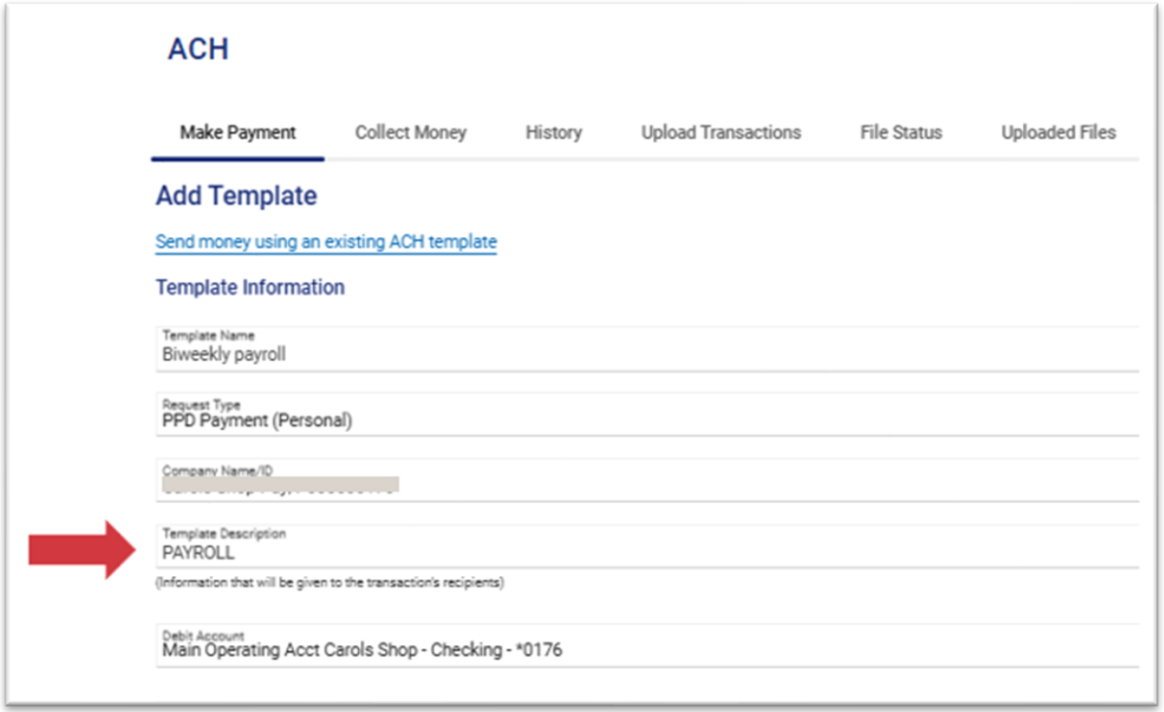
Standard Company Entry Descriptions

Payroll and E-Commerce Descriptions: Establishes standardized descriptions for payroll (“PAYROLL”).

NACHA ACH Payment Updates March 20, 2026

Standardized Entry Descriptions for Payroll
Promotes standardization- participants can easily identify the purpose of the transactions and improves the quality of information.

- Payroll- Standardization to identify payroll payments helps support practices intended to reduce the incidence of fraud involving payroll redirection



HARBOR

Fraud Monitoring as an ACH Originator June 19, 2026

ACH Originators should implement risk-based procedures to identify transactions that may be unauthorized. At a minimum, they should address the following areas:

Unauthorized Payments

- Safeguard online banking credentials, which can be compromised through malware.
- Maintain separate email accounts for work and personal use.
- Avoid clicking on links until verifying legitimacy directly through a known phone number or the vendor's official website.

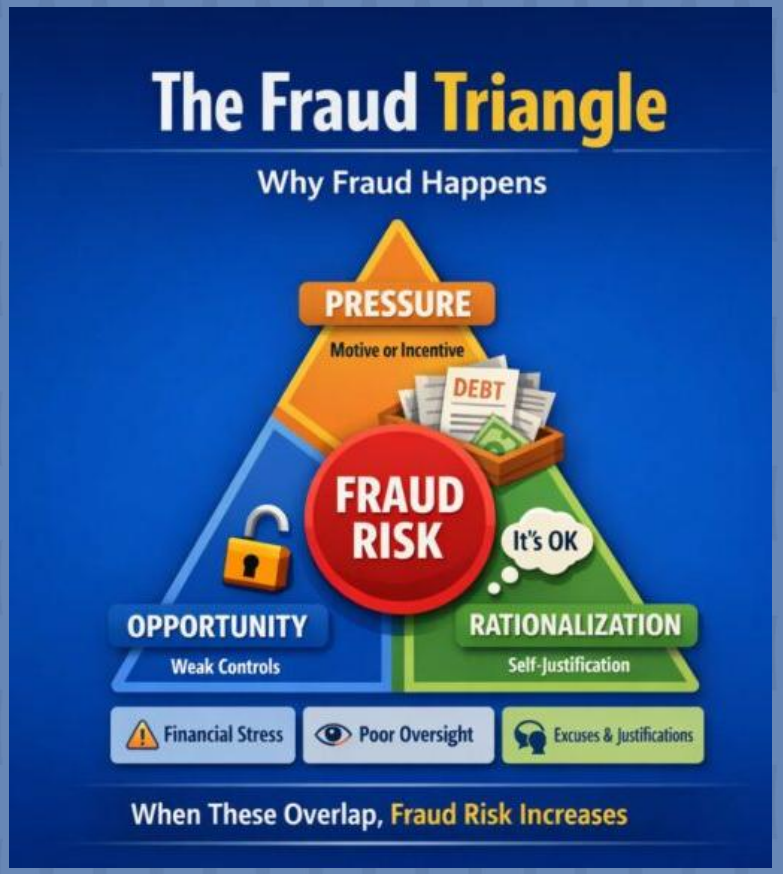
Authorized Payments Made Under False Pretenses

- Independently confirm any vendor-related account changes or payment instructions by calling a trusted phone number, as email compromises and impersonation attempts can make fraudulent requests appear authentic.

Dedham Savings

Rule Change Questions?

Fraud Awareness

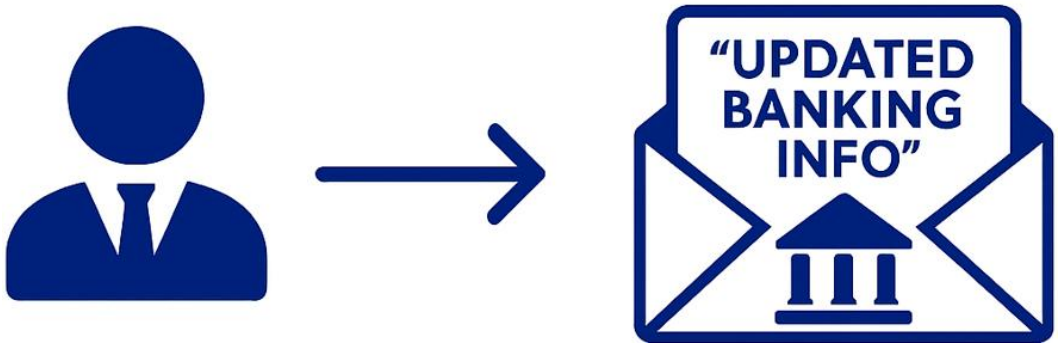


Five Common Fraud Tactics

1. Business Email Compromise (BEC) & Payroll/Vendor Impersonation

Impersonation of trusted parties to request payments or bank-detail changes. Fraudsters attempt to redirect payroll or vendor payments to fraudulent accounts.

- **Red flags:** Urgent requests, spoofed domains, off-hours messages; “updated banking info,” slight name/email variations.
- **Control:** Callback verification of all payment-detail changes + dual control for payee edits.



Five Common Fraud Tactics Cont.

2. Bank Impersonations

Fraudsters impersonate the bank, IT support, or Fraud department to trick clients into providing credentials, moving funds, verify ACH & Wire payments.

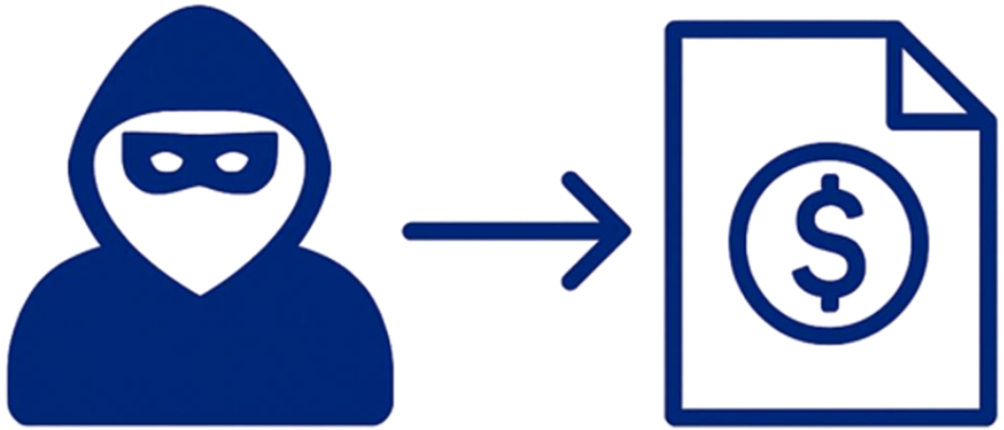
- **Red flags:** Requests to “verify” account numbers, login credentials, tokens, or ACH/Wire instructions.
- **Control:** Never share credentials; verify bank-related calls using a known, trusted phone number.

Five Common Fraud Tactics Cont.

3. Account Takeover (CATO)

Criminals use stolen credentials to originate unauthorized ACH transactions.

- **Red flags:** New templates, unusual timing or velocity.
- **Control:** Strong MFA + daily monitoring + Training



Five Common Fraud Tactics Cont.

4. Credit-Push Fraud (False Pretenses)

Victims are coached into authorized transfers under deception.

- **Red flags:** “Verify/move money,” mismatched accounts, first-time payees.
- **Control:** Anomaly monitoring + employee/social engineering awareness.

Five Common Fraud Tactics Cont.

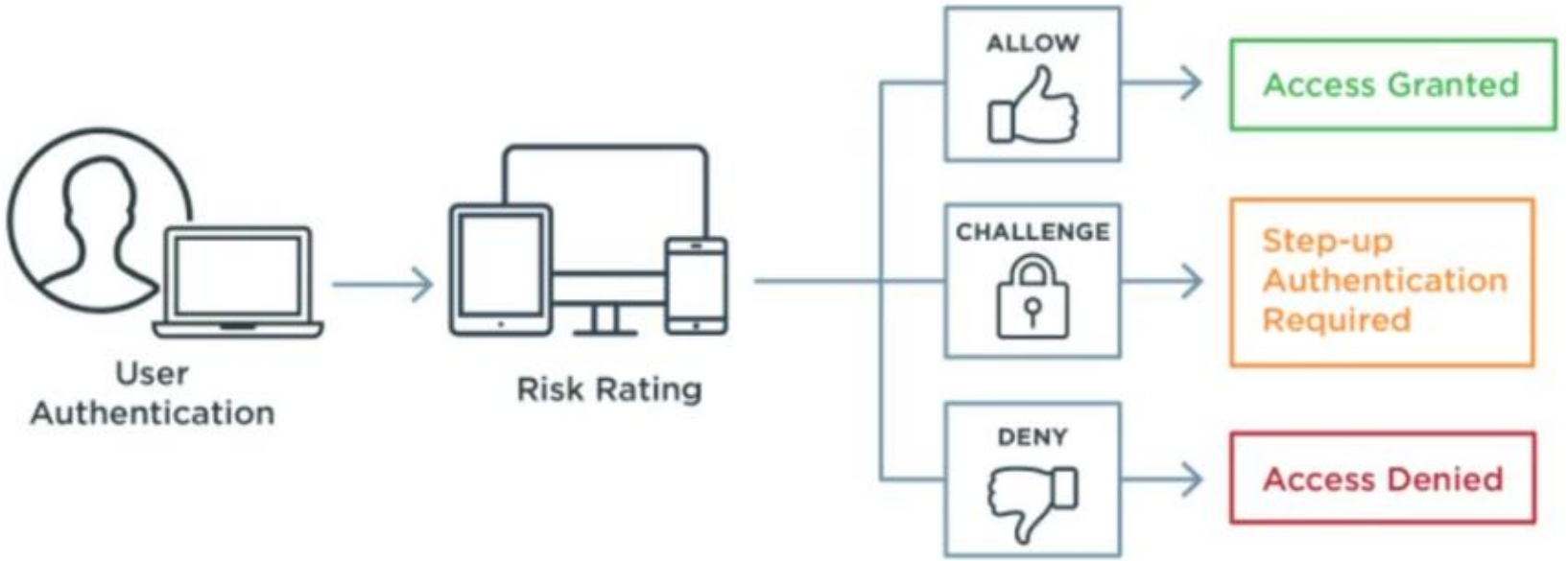
5. Fake Invoices / Purchase Order Scams

Fraudulent invoices that look legitimate but direct funds to criminals.

- **Red flags:** Slightly altered vendor names, new routing numbers.
- **Control:** Independent invoice validation + segregation of duties.

HARBOR

7 Controls for Preventing & Detecting Corporate Account Takeover



Dedham Savings

HARBOR

7 Controls for Preventing and Detecting Corporate Account Takeover

Implement Segregation of Duties: Ensure that payment initiation and payment approval are performed by separate authorized users to reduce the risk of unauthorized transactions.

Conduct Daily Account Monitoring: Review account activity every business day and immediately contact the bank if any unusual, unexpected, or suspicious transactions are identified.

Provide Continuous Employee Awareness Training: Educate employees on how to recognize potential fraud attempts through email, phone calls, text messages, faxes, and mailed correspondence.

Dedham Savings

HARBOR

7 Controls for Preventing and Detecting Corporate Account Takeover Cont.

Use Secure Communication Channels: Always utilize encrypted emails or otherwise secure methods when exchanging sensitive account or payment-related information with vendors or third parties.

Verify All Payment Instruction Changes: Train staff to independently validate any requests to modify vendor account details or payment instructions, especially those that appear urgent or secretive.

Protect Online Banking Credentials: Instruct employees never to disclose login credentials or account information to anyone—including individuals claiming to represent the bank.

Follow the Business Incident Response Plan: Leverage the incident response plan provided by the bank to quickly identify, escalate, and mitigate potential fraud events.

Dedham Savings

Employee Training Recommendations to Prevent Phishing

Train Your Employees to be Alert for Phishing Attempts

Email Phishing	An employee receives an email claiming to be from a known vendor.	Red Flags: •Slightly altered sender address (e.g., @vend0r-pay.com instead of @vendor-pay.com) •Message states the vendor "updated their banking information" •Attached "urgent" PDF or invoice instructing immediate payment •Links directing the user to a login page asking for credentials

"See Something.....Say Something"

Business Email Compromise/CEO Fraud	An employee receives an email that appears to be from an executive requesting an urgent wire transfer before "end of day."	Red Flags: •Language that creates urgency or secrecy •Sent during non-business hours •Request deviates from normal approval procedures

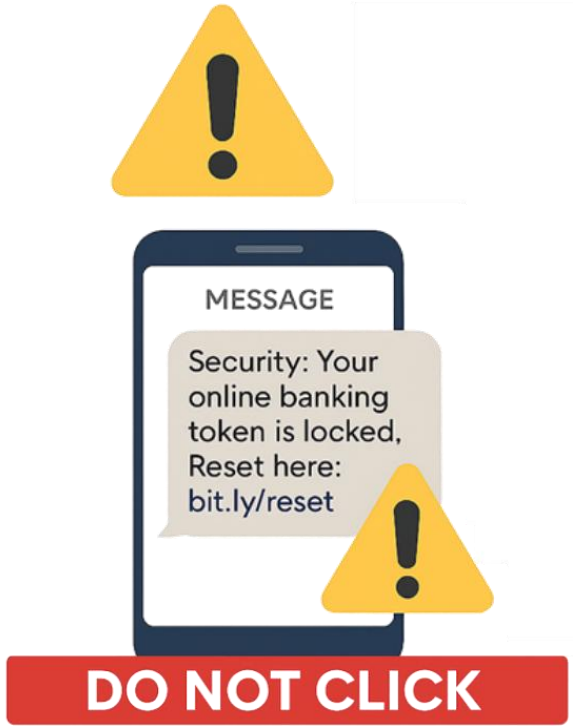
Be Alert, Aware and Prepared....Don't be a Victim

Four Common Phishing Attempts

1. **Text Message (SMS) Phishing (Smishing)** A staff member receives a text claiming their online banking token is “locked” and they must click a link to reset it.

Red flags:

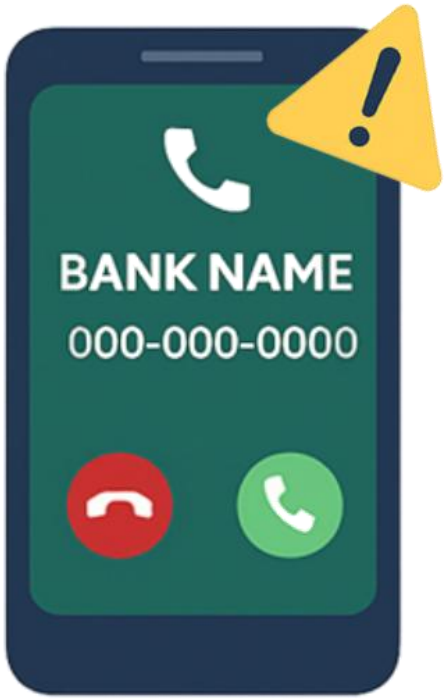
- Unexpected security alert
- Shortened URL (e.g., bit.ly)
- Requests credential verification



Four Common Phishing Attempts

2. Phone-Based Social Engineering (Vishing)

A caller claims to be from IT support or the bank's fraud department.

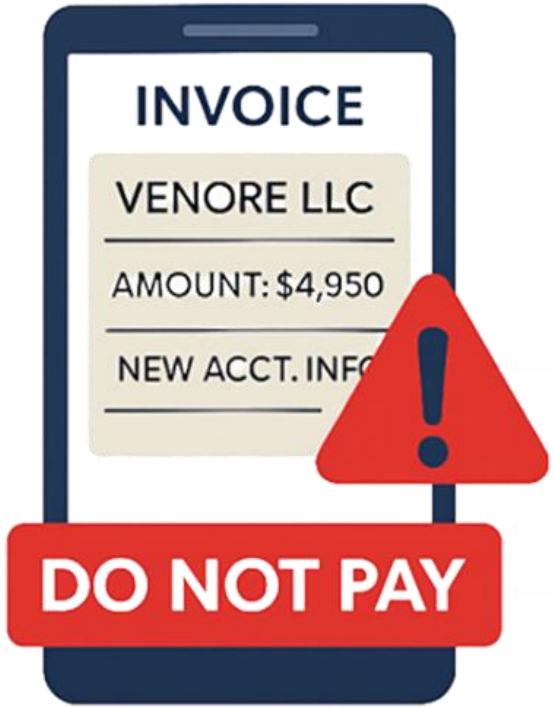


Red flags:

- Caller pressures employee to "confirm login information"
- Claims of suspicious activity that require immediate action
- Caller ID spoofing matching the bank's number

Four Common Phishing Attempts

3. Fake Invoice or Purchase Order Scam Accounts Payable receives an invoice for services that were never authorized or performed.



Red flags:

- Vendor name resembles a real vendor but is slightly different
- New banking instructions included on the invoice
- Invoice amount slightly under approval threshold

Four Common Phishing Attempts

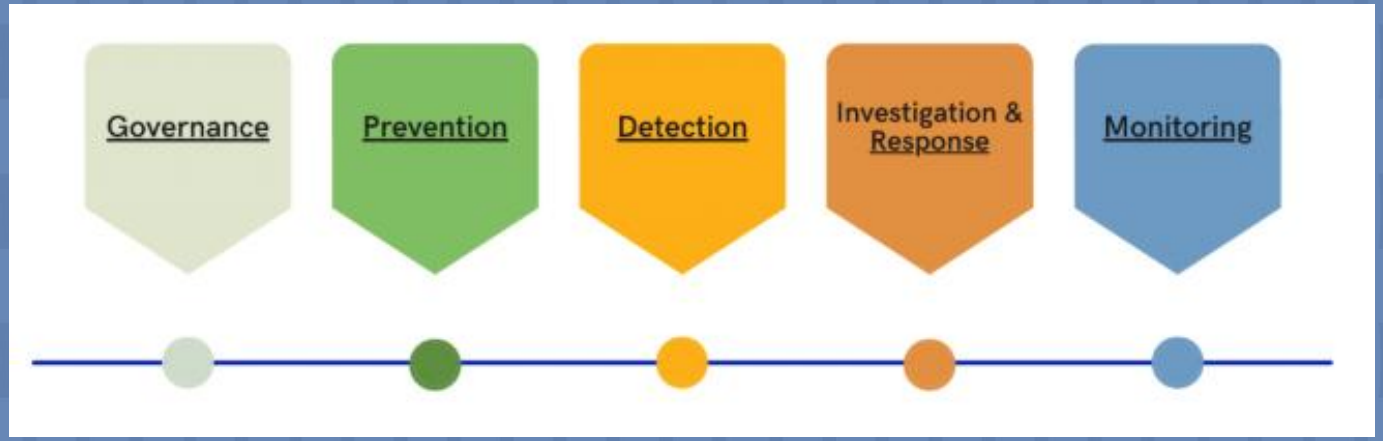
4. Malware-Based Phishing (Attachment Attack)

Employee receives an email with a ZIP, PDF, or Excel attachment labeled “Updated ACH File” or “Payroll Report.”

Red flags:

- Unexpected attachment
- Macros required to open the file
- Poor grammar or formatting

Tools to Reduce Fraud Risk



HARBOR

Operational Tools to Reduce Fraud Risk

ACH & Check Positive Pay: Enables monitoring of check payments and ACH debits, allowing inappropriate or suspicious items to be identified and returned when necessary.

Secure Email to Vendors: Using password-protected, secure email reduces the risk of unauthorized access to sensitive documents, when possible.

RSA Token at Login: Adds an extra authentication layer, reducing the likelihood of unauthorized access. Users must have both their RSA token and personal PIN.

Dual Control for Payment Processing: Separating the roles of payment initiator and approver significantly lowers risk if a user's credentials become compromised.

Online Banking Alerts: Immediate alerts help ensure that most payments can be reversed when the bank is notified promptly.

HARBOR

Cybersecurity Insurance: A Financial Safety Net for Business

Offsets direct financial losses resulting from fraudulent activity.

Funds comprehensive forensic investigations and legal counsel.

Reimburses expenses for customer notification and identity monitoring.

Mitigates the impact of regulatory fines and penalties.

Facilitates rapid business recovery to minimize operational downtime.

Dedham Savings

Additional Resources

For additional fraud-prevention tools, educational resources, and up-to-date best practices, visit:

https://www.dedhamsavings.com/nacha-updates/

https://www.nacha.org/rules/risk-management-topics-fraud-monitoring-phase-2

Contact Information Dedham Savings

Treasury Services Team
treasurymanagement@dedhamsavings.com
781.320.1115

Ed Skou
Directory of Treasury Mgt.
eskou@charlesbridgegroup.com

Contact Information Harbor IT

Rolin "Bud" Peets, CISSP | CIPM
Chief Protection Architect
rolin.peets@harborit.com

John D. Flory III
Cyber Security Practice Lead
John.flory@harborit.com

Questions?

HARBOR

Thank You

Dedham Savings