craft bank

1st QUARTER 2025

PAYMENTS NEWSLETTER

FOR TREASURY CUSTOMERS

Upcoming Changes to Wire Transfers

ISO 20022 is a global payment messaging standard implemented by the International Organization for Standardization. The ISO 20022 project is a strategic initiative by the Federal Reserve to align the Fedwire Funds Service message format with a global standard that can improve transaction processing efficiency and promote interoperability among high-value payment systems globally.

ISO 20022 will enable better structured and more granular data end-to-end to be carried in payments messages. Wire transfers will continue to be processed through the Fedwire system, but there are terminology changes in the transaction flow.

Below are common terms to become familiar with prior to the implementation:

Current Fedwire Term	ISO 20022 Reference Term
Originator	Debtor
Originating Financial Institution	Debtor Agent
Sending Financial Institution	Instructing Agent
Beneficiary	Creditor
Beneficiary Financial Institution	Creditor Agent
Receiving Financial Institution	Instructed Agent

We will continue to provide information about ISO 20022 Implementation. For more information and to view prerecorded webinars, visit the following sites:

https://www.frbservices.org/resources/financial-services/wires/iso-20022-implementation-center

https://www.frbservices.org/binaries/content/assets/crsocms/resources/financial-services/mystandards-access-instructions.pdf.

Phishing Threat Response - Unpaid Tolls

Have you received a text about unpaid tolls? An example of the scam text people may receive reads as follows: “Pay your FastTrak Lane tolls by February 13, 2025. To avoid a fine and keep your license, you can pay at https://ezdrivema.com-xlk.vip/i/. (Please reply Y, then exit the text message and open it again to activate the link, or copy the link into your Safari browser and open it.)”

The Toll Roads do not send text messages to non-accountholders. If you receive a phishing text, please file a complaint at ReportFraud.FTC.gov.

One of the best ways to prevent phishing is to know how to spot phishing emails and texts. While every email may look a little different, there are red flags to help you spot phishing. Common warning signs of phishing include:

- Urgent or emotionally appealing language
- Untrusted shortened URLS
- Incorrect email addresses or links
- Unsolicited messages and attachments

Another great way to ensure your device is protected from phishing is to keep your operating system up to date. Most times, operating system updates include essential security patches to keep your device safe. This can help protect you from phishing-related threats such as malware. When a phishing email/text is identified, it should be reported immediately. By

fostering awareness and maintaining a vigilant response strategy, organizations can effectively reduce the impact of phishing attacks.

Preparing for Upcoming Nacha Rules Changes

You may recall from previous issues that all participants in the ACH network will be required to have fraud controls in place. If you are concerned on where to begin, we have a solution for you! Check out the checklist below and document all controls you have available.

Inventory Checklist of Fraud Controls

Effective Date: March 20, 2026

1. Authentication and Access Controls

[ ] User Access Management: Restrict access to ACH origination systems based on job roles and responsibilities.

[ ] Session Timeouts: Automatically log out users after periods of inactivity.

[ ] IP Address Whitelisting: Allow access only from approved IP addresses.

2. Fraud Detection and Monitoring Systems

[ ] Transaction Monitoring: Implement systems to monitor transactions in real time or near real time for anomalies.

[ ] Velocity Controls: Set thresholds for the number or value of transactions allowed within a specified time frame.

[ ] Geolocation Monitoring: Detect transactions originating from unusual or high-risk geographic locations.

3. Customer Validation and Account Verification

[ ] Prenotification Entries (Pre-Notes): Send zero-dollar test transactions to verify account details before initiating live payments.

[ ] Micro-Deposits: Send small test deposits and require customers to confirm the amounts to verify account ownership.

4. Data Security and Encryption

[ ] Data Encryption: Encrypt sensitive data in transit and at rest, including account numbers and personal information.

[ ] Network Segmentation: Isolate ACH systems from other parts of the network to reduce vulnerability to cyberattacks.

5. Fraud Alerts and Notifications

[ ] Threshold Alerts: Automatically trigger alerts for transactions exceeding predefined thresholds.

[ ] Suspicious Activity Alerts: Notify administrators of unusual activity patterns or failed login attempts.

[ ] Customer Alerts: Inform customers of initiated transactions and allow them to confirm or dispute them.

6. Training and Awareness

[ ] Employee Training: Train employees on fraud risks, red flags, and compliance requirements for ACH origination.

7. Incident Response and Reporting

[ ] Fraud Incident Response Plan: Develop and maintain a documented plan for responding to suspected fraud incidents.

[ ] ODFI Communication: Establish protocols for reporting fraudulent transactions to us promptly.

[ ] Customer Notification: Notify impacted customers of suspected fraudulent activity and provide steps to mitigate risks.

[ ] Post-Incident Review: Conduct a root cause analysis of fraud incidents and update controls to prevent recurrence.

8. Audit and Testing

[ ] Regular Audits: Perform periodic internal and external audits of fraud controls and ACH origination processes and adjust as necessary.

Standard Company Entry Description

Effective Date: March 20, 2026

Your company uses the Company Entry Description field to describe the purpose of the payment being sent to your receiver.

Currently, the ACH Rules dictate what goes in this field in certain circumstances (e.g., “REVERSAL” if you are reversing an erroneous payment).

This amendment requires companies initiating (1) PPD credits to Consumers related to wages, salaries, or similar types of compensation to input a description of “**PAYROLL**” in the Company Entry Description and (2) e-commerce/online retail purchases (WEB debits) to use “**PURCHASE**”. In order to prepare for the changes, review your software and online banking to ensure the proper description is used.

If you have questions about the newsletter or would like more information on fraud mitigation tools and treasury service offerings, please contact:

Craft Bank Support at 678-736-5060 or support@craft.bank