craft bank

SUMMER 2024

PAYMENTS NEWSLETTER

FOR TREASURY CUSTOMERS

2024 ASSOCIATION OF FINANCIAL (AFP) PROFESSIONALS FRAUD STUDY

Each year, AFP publishes its annual payment fraud study. Even given the controls and processes businesses put in place, fraudsters continue to advance their scams by devising different methods to trick employees at businesses and their consumers.

Some key findings from this report include:

- 80% of organizations reported having been targets of payments fraud activity in 2023, an increase from 65% in 2022.
- Checks continue to be the payment method most susceptible to fraud, as reported by 65% of respondents.
- 70% of organizations using checks have no immediate plans to discontinue their use.
- For the first time since AFP began conducting the payments fraud survey, ACH credits have surpassed wires as the most vulnerable payment type for BEC fraud.
- 63% of organizations experienced some form of BEC in 2023.

Source: 2024 AFP® PAYMENTS FRAUD AND CONTROL SURVEY REPORT

BUSINESS SCAMS AWARENESS

You have heard about consumer scams online or on the news, you've read a story about an elderly person whose retirement funds were drained by a pretend tech support representative, or you've seen something on the news about thieves stealing checks out of mailboxes. These types of scams continue to be a threat to individuals and businesses. What you may not realize is that many businesses find themselves to be the victim of this fraud. In many cases, businesses don't recognize the signs of fraud and don't know what's happening until it's too late. That's why being vigilant and ready to outsmart those fraudsters is more important than ever.

What types of fraud should your business be on the lookout for?

PHISHING ATTACKS

Phishing attacks use fraudulent emails, text messages, phone calls, or websites to trick people into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime. In a typical phishing attempt, a fraudster pretends to be someone you trust, like a colleague, boss, known vendor, authority figure, or representative of a well-known brand. The hacker sends a message directing the victim to pay an invoice, open an attachment, click a link, or take some other action.

BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) scams occur when a fraudster impersonates a company executive or trusted vendor to manipulate employees into transferring funds or sensitive information under false pretenses. BEC scammers use various tactics like social engineering, email spoofing, and gathering information about organizations to exploit weaknesses.

TIPS FOR FRAUD PREVENTION AND DETECTION

- **Never rely solely on an email for requesting or authorizing a payment**.
- Implement check and balance process for employees with access to create and approve payment transactions.
- Educate employees on threats posed by phishing attempts and how to identify them.
- Reconcile transactions daily and quickly request a return of any unauthorized debits.
- If you notice fraudulent activity, it's important to act quickly and contact your treasury sales and support team.

- Implement policies for providing appropriate verification of any changes to existing invoices, bank deposit information, and contact information.
- Research charities and see more giving tips at Give.org.

These controls can significantly reduce the risk of fraud within your company. By adopting and following these practices, you can strengthen your internal controls and protect your assets from fraudulent activities.

NEW ACH RULES CHANGES IN EFFECT

On March 15, 2024, Nacha passed 15 new Rules changes surrounding ACH risk management. New Nacha Operating Rule changes are meant to reduce the incidence of frauds, such as business email compromise (BEC) or impersonation schemes, which make use of credit-push payments. The new Rules will impact ACH originators and establish a base-level for ACH payment monitoring on all parties in the ACH Network (except consumers). The new Rules follow the flow of a credit-push payment to promote the detection of fraud from the point of origination through receipt at an account at the RDFI.

Effective June 21, 2024

The following Rule changes take effect June 21, 2024:

- **General Rule Definitions for WEB Entries**: This rule rewords the WEB general rule and definition in *Article Eight* to make it clearer that the WEB SEC Code must be used for all consumer-to-consumer credits regardless of how the consumer communicates the payment instructions to the Originating Depository Financial Institution (ODFI) or P2P service provider.
- **Definition of Originator**: Clarifies changes and alignments to the definitions of Originator to include a reference to the Originator's authority to credit or debit the Receiver's account and that the Rules do not always require a receiver's authorization (e.g., reversals, reclamations, person-to-person entries).
- **Originator Action on Notification of Change (NOC):** Provides Originators with discretion to make NOC changes for a Single Entry, regardless of the SEC Code.
- **Data Security Requirements**: Clarifies that, once a covered party meets the volume threshold for the first time, the requirement to render account numbers unreadable remains in effect, regardless of future volume.
- **Use of Pre-Notification Entries**: Aligns the pre-note rules with industry practice by removing language that limits pre-note use to prior to the first credit or debit entry.
- **Clarification of Terminology ("subsequent entries")**: Replace references to "subsequent entry" in various sections with synonymous terms to avoid any confusion with the new definition of "subsequent entry."

Effective October 1, 2024

The following Rule changes take effect October 1, 2024:

- **Additional Funds Availability Exceptions**: Provides RDFIs with an additional exemption from the fund's availability requirements including credit ACH entries that the RDFI suspects are fraudulent.
- **Codifying Use of Return Reason Code R17**: Allows RDFIs to return an entry believed to be fraudulent using Return Reason Code R17.
- **Expands Use of ODFI Request for Return/R06:** Expand the permissible uses of the Request for Return Reason Code (R06) to allow an ODFI to request a return from the RDFI for any reason.
- **RDFI Must Promptly Return Unauthorized Debit:** Requires that when returning a consumer debit as unauthorized in the extended return timeframe, the RDFI must do so by the opening of the sixth Business Day following the completion of its review of the consumer's signed Written Statement of Unauthorized Debit (WSUD).
- **Timing of Written Statement of Unauthorized Debit (WSUD):** Allows a WSUD to be signed and dated by the Receiver on or after the date on which the Entry is presented to the Receiver, even if the debit has not yet been posted to the account.

We will continue to update our treasury clients on upcoming rules changes and how it will impact you as an originator.

For more information on fraud mitigation tools and service offerings, please contact:

support@craft.bank

678-736-5060