4th QUARTER 2023

PAYMENTS NEWSLETTER

FOR TREASURY CUSTOMERS

CHECK FRAUD ALERT FOR BUSINESSES: BE AWARE AND ACT FAST

Many businesses continue to write checks and receive checks as part of their accounts payable and receivable procedures. This payment method is one of the oldest forms of payment channels; however, in today's evolving fraud landscape, check fraud has significantly increased, making businesses take a pause and rethink how they pay and get paid.

Feds warn of 'surge' in check washing scams

US postal inspectors recover $1 billion in counterfeit money orders and checks each year

Mail thefts of high volume, including from blue collection boxes, rose from 38,500 in FY 2022 to more than 25,000 in the first half of FY 2023, the Postal Service said.

HOW DOES CHECK FRAUD HAPPEN?

Check fraud can take on several types of schemes and can be the result of an internal employee or a fraudster on the outside. Altered, forged, and counterfeit checks are the most common types of check fraud.

Altered checks are physical checks that have been stolen (either through the mail or other means) followed by an alteration of the payee. With altered checks, a fraudster obtains the business's physical check and alters the information. If your business writes physical checks and places these checks in the mail, you may open yourself up to unnecessary risks. Fraudsters may intercept incoming or outgoing checks that are meant to pay a vendor or employee. In some cases, the fraudster will "wash" the physical check, which means the fraudster uses a chemical to remove the written information (other than the signature) from the check and inserts a new payee.

Counterfeit checks are another type of a check fraud scheme that results in fraudsters using a check that looks like it is an authentic check written by a business. In addition to altering the physical check fraudsters intercept, they can change other information on the check — such as the authorized signature, account number, routing, and transit numbers — to create counterfeit checks in the future.

INTERNAL CHECK FRAUD

Sometimes, check fraud may be the result of an internal employee with access to the company's account information. Typically, this type of fraud occurs when one individual is responsible for all accounts payable and receivable processes, and there are no dual control procedures in place. This is common even with trusted, long-time employees.

DON'T DELAY REPORTING FRAUD

Report fraud as soon as you think your business has been a victim. Never wait to report fraud or even a potential fraud event. The quicker you report it, the better we will be able to assist you in recovery efforts.

WHAT TOOLS ARE AVAILABLE

Businesses have fraud tools to choose from and should ensure they are prepared based on the significance of check fraud. One of the main tools available to businesses is check positive pay.

Positive pay protects you from checks presented for payment that may include an altered payee, dollar amount, or check number so you can determine which checks should be paid or rejected. With increased check fraud and corporate account losses, this tool benefits you and protects your money.

REMINDER ABOUT REINITIATING ACH ENTRIES: KNOW YOUR RESPONSIBILITIES

There are Nacha requirements when originating outgoing ACH entries that you need to ensure are part of your daily procedures when receiving a return from the receiving financial institution. The first thing to know is that as an ACH Originator, you can only reinitiate an entry that was returned for the following reasons:

1. Insufficient or uncollected funds, which can be reinitiated two times following the return of the original entry.

2. The entry was returned for a stop payment and the reinitiation of the entry was authorized by the Receiver.

3. The ACH Originator corrected the entry with the Receiver by obtaining another authorization.

If it is a Redeposited Check Returned Entry, there are reinitiation rules that apply, so refer to the Nacha Rules.

Deadline for Reinitiating Entries

When reinitiating any entry, understand that reinitiation must occur within 180 days after the Settlement Date of the Entry.

HOLIDAY FRAUD AWARENESS: EDUCATE, BE ALERT, AND PROTECT YOUR MONEY

During the holidays, businesses experience a significant rise in fraudsters attempting to trick or successfully tricking them into surrendering their online credentials and/or falling for scams resulting in significant monetary losses. Based on the increased risks during the holiday season, it is a great time to pull all your employees together, train them on these scams, and educate on how to stop fraud before it happens. Below are some simple but effective tips to share with your teams to stay vigilant and protect your money during the holiday season:

- Understand these attacks can come via email, phone calls, faxes, or letters in the mail

- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, payment methods (e.g., ACH to wire, checks to wires), or pressure to act quickly or secretively

- Review your account daily and contact us if you have any suspicion of fraud.

- Initiate payments using dual controls.

- Do not provide password, username, authentication credentials, or account information when contacted or through any other means.

- Do not provide nonpublic business information on social media.

- Avoid free web-based email accounts for business purposes. A company domain should always be used in business emails.

HAVE A SAFE AND HAPPY HOLIDAY!