epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

Nightmare on Check Fraud Street

by Marcy Cauthon, AAP, AFPP, APRP, NCP, Senior Director, On-Demand Education

While many think paper checks have vanished into the shadows, they still represent about one-third of all business-to-business (B2B) transactions, according to the Association of Financial Professionals.

Unfortunately, we are seeing a chilling surge in check fraud schemes, with check fraud being the largest source of illicit proceeds in the United States, according to the Financial Crimes Enforcement Network (FinCEN). Therefore, it's critical that your business recognizes the red flags before they come to light, especially when it's too late.

Check fraud happens when criminals produce fake checks or steal mail containing personal checks, business checks and any government checks. These checks are then altered or counterfeited, physically or digitally, to allow different payees or larger amounts.

It's important to understand the difference between an altered check and a counterfeit one. It states in the Uniform Commercial Code (UCC) that an alteration "must" occur on the original paper check that your business issued. For example: your business issues a check, a criminal gets hold of it, washes it with chemicals and then writes or types new information on it. Conversely, a counterfeit happens when a criminal uses information from a legitimate check your business issued to create new checks on different check stock. While there are many types of check fraud, alterations and counterfeits are two of the most common.

To keep your business from being spooked by check fraud, watch for these common red flags:

- A check or an order of checks was never received.
- Checks are missing from your check stock.
- A check your business mailed to an intended recipient never arrives.
- A check that was issued has not cleared the bank account after several months.

Check fraud is a spooky reality. While there are steps to recover funds after it occurs, prevention is always the best defense. Some measures to consider include:

- **Positive Pay**—Most financial institutions offer a positive pay product for checks and/or ACH transactions. This two-fold fraud protection service

helps detect unauthorized checks and ACH debit transactions. As checks are issued, you upload a file with their details into online banking. When checks clear, Positive Pay matches this information against your file. Any checks that don't match are held as an "exception item" for your company to pay or return. You can ask your financial institution if this is a service they offer for businesses.

- **Remote Deposit Capture (RDC)**—Many financial institutions offer some type of RDC, which allows you to deposit checks digitally without ever leaving your business. It also includes comprehensive review and reporting capabilities based on individual deposits, check numbers, item types and routing numbers.
- **Digital Payment Options**—Consider using a digital payment option like ACH or card payments instead of relying on paper checks. Unlike checks, digital payments cannot be intercepted in the mail or physically altered, reducing the risk of fraud. They also streamline the payment process by saving time, cutting down on travel and providing greater convenience for both your business and the recipient.

Protect your business from the ghouls and goblins of check fraud with these suggested precautions:

- **Employee Safeguards**—Unfortunately, check fraud can sometimes originate within your organization. Consider separating duties so the person signing checks isn't the same person reconciling accounts, adding dual oversight in accounts payable or even introducing occasional surprise audits to strengthen controls.
- **Physical Security Measures**—It may be wise to keep check stock locked in a secure location, ideally somewhere with a frequently changed access code or combination. You may also want to take steps to secure your mailroom, especially if your business mails out checks.
- **Trackable Shipping**—When mailing checks, opt for a trackable shipping method and monitor each item until you have delivery confirmation. Requiring a signature upon receipt can add another layer of protection.

Trying to recover funds after check fraud is like navigating a haunted maze—complicated, frustrating and full of unexpected twists. That's why reconciling your accounts regularly and often is key. If you suspect check fraud, acting quickly gives you the best chance of recovery. Notify your financial institution immediately if something is amiss. Keeping thorough records of transactions, especially if payments were prompted by an email or phone call, can also provide valuable evidence if the situation escalates to legal action.

If you'd like more information on what options are available to your organization to reduce fraud, reach out to your financial institution.

Ghost Your NOCs and They'll Come Back to Haunt You

by Shelly Sipple, AAP, AFPP, APRP, NCP, Senior Director, Certifications & Continuing Education

If your business originates ACH payments, you may have come across something called a "Notification of Change," or NOC, and thought, "Not Our Concern." But beware—ignoring NOCs can come back to haunt you, and here's why.

What Are NOCs?

NOCs are messages sent through the ACH Network to alert you that something in your payment instruction needs to be updated, such as an incorrect routing number, account number or transaction code. These updates help ensure your payments continue to process correctly and on time, keeping you from being haunted by failed transactions.

How Do NOCs Work?

Let's walk through a common scenario:

You send an invoice to a customer, and they authorize you to pull the payment from their account via ACH. You initiate the transaction, but when it arrives at the customer's financial institution, it hits a snag. Maybe you coded the payment for a checking account, but the customer only has a savings account.

At this point, the receiving financial institution (called the RDFI) has two choices:

1. Return the payment to you (a hassle for both you and your customer), or
2. Post the payment and send you an NOC to let you know how to correct the payment information for future use.

The second option is more customer-friendly and ensures you get paid. But it also means you have to take action.

What Are You Required to Do?

According to the *ACH Rules*, your financial institution must notify you within two banking days of receiving an NOC related to one of your payments. Notification may come by telephone, secure email or as a report in your online banking portal. Once notified, you must make the specified change(s) within six banking days or before you send your next ACH entry for that customer, whichever comes later.

If you don't expect to send another payment to that customer, no need to worry. But if they're a repeat customer (and hopefully they are!), you need to update the information in your system to avoid future issues.

Why Acting on NOCs Matters

Ignoring NOCs can turn into a nightmare. Responding to NOCs isn't just about compliance; it's smart business. Keeping your payment information up to date helps you:

- Reduce errors
- Avoid rejected payments
- Ensure prompt payment
- Maintain accurate records
- Provide better customer service

And let's face it—no one wants to chase down failed transactions or deal with late payments lurking like a shadow.

Stay Ahead of the Game

To stay compliant and efficient, follow these best practices:

- Monitor for NOCs daily
- Apply changes as soon as possible
- Document your updates and compliance efforts

Still Have Questions?

Reach out to your financial institution or visit epcor.org/corporateuser for more compliance resources tailored to corporate ACH users. Don't let NOCs haunt your business—stay proactive and keep your payments running smoothly.

Don't Let ACH Risk Haunt You!

EPCOR's *Third-Party Sender Bundle* arms your team with the tools to navigate the ACH Network safely. With three live webinars, nine on-demand courses and three publications, you'll uncover need-to-know insights of your role, master the *ACH Rules* and build a risk-proof ACH Management Program. Keep surprises—and fraud—out of your payments.

Don't Let New Rules Changes Creep Up on Your Organization

by Trevor Witchey, AAP, APRP, NCP, Senior Director, Payments Education

By March 20 or June 19, 2026 (*Phase 1*, starting March 20, 2026, applies to non-consumer originators and third-parties with 2023 ACH origination volume of 6 million or more. *Phase 2*, starting June 19, 2026, applies to all remaining non-consumer originators and third parties), ACH Originators must establish and implement risk-based processes and procedures reasonably intended to identify ACH Entries initiated due to fraud. This is part of Nacha's new Origination Fraud Monitoring Rule, designed to keep fraudsters from initiating ACH payments due to unauthorized access or inducing an Originator to send something under false pretenses. If you're unsure how the requirements apply to your organization, check with your financial institution for guidance.

These procedures should be tailored to your role in authorizing and transmitting entries and must be reviewed and updated at least annually to keep pace with evolving fraud risks.

Where to Focus Your Efforts

Most ACH payments are sent to the same Receivers, such as payroll, vendors, utilities, etc., so concentrate your controls on atypical situations that could hide fraud, such as:

- **Brand-New Receivers:** Before initiating a credit, verify the legitimacy of the Receiver. This includes checking identification, performing background checks and confirming signers are authorized representatives. Obtain their authorization legitimately, while ensuring sensitive account information is transmitted securely and/or through an encrypted fashion.
- **Existing Receivers with Account Changes:** If a long-time Receiver sends new account details unexpectedly (especially via email, text or fax), treat it as a red flag. Always verify using known contact information on file (not from an email), not the message that initiated the change. Apply Know-Your-Customer (KYC) practices to confirm the request is valid.

These are the moments when your fraud detection procedures should kick in.

Two Key Compliance Points

- **Point of Transmission:** Under *ACH Rules Section 1.7*, sensitive data like account and routing numbers must be encrypted during transmission. Originators transmitting such data over unencrypted email are at risk and in violation. You're also more vulnerable to business email compromise. Implement encryption and consider tokenization to keep data safe from lurking fraudsters.
- **Point of Authorization:** Per *ACH Rules Subsection 2.3.1*, Originators must obtain valid, legally compliant authorization from the Receiver. This means the method must clearly link the Receiver to the consent. Email alone isn't enough, as anybody could initiate an email and it does not fit legal requirements for an authorization. Instead, use traceable methods like HR systems, written authorizations or voided checks to protect both parties.

Why It Matters

According to the FBI's IC3 2024 report, business email compromise was the second most common fraud type (behind investment fraud, which has escalated recently). Meanwhile, a Center for Payments survey identified "Authorized User was Manipulated" as the top emerging threat. Regardless of size, Originators must document and follow clear procedures to meet the Rule's requirements and reduce fraud exposure.

Reach out to your financial institution to discover the tools they offer to strengthen your fraud defenses. Having more than one set of eyes makes it much harder for fraudsters to succeed—don't let invisible threats haunt your payments.

Catch the ghouls before they strike! Watch EPCOR's Monitoring for Fraud *Did You Know* video for bone-chilling tips on spotting unauthorized activity and be sure to subscribe to EPCOR's YouTube channel, EPCORPymnts, to stay in the know and keep your payments safe from hidden threats.

STAY INFORMED.

Check out this year's ***2025 ACH Rules Update for Corporate Originators and Third-Party Senders*** to understand the latest requirements and best practices.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
800.500.0100 | 816.474.5630