BANK of BELLEVILLE · CLINTON COUNTY MADISON COUNTY · MONROE COUNTY
Smaller Bank · Bigger Service · Stronger Community

epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

2022's Top Third-Party Sender Audit Findings

by Matthew T. Wade, AAP, APRP, CPA, Manager, Advisory Services, EPCOR

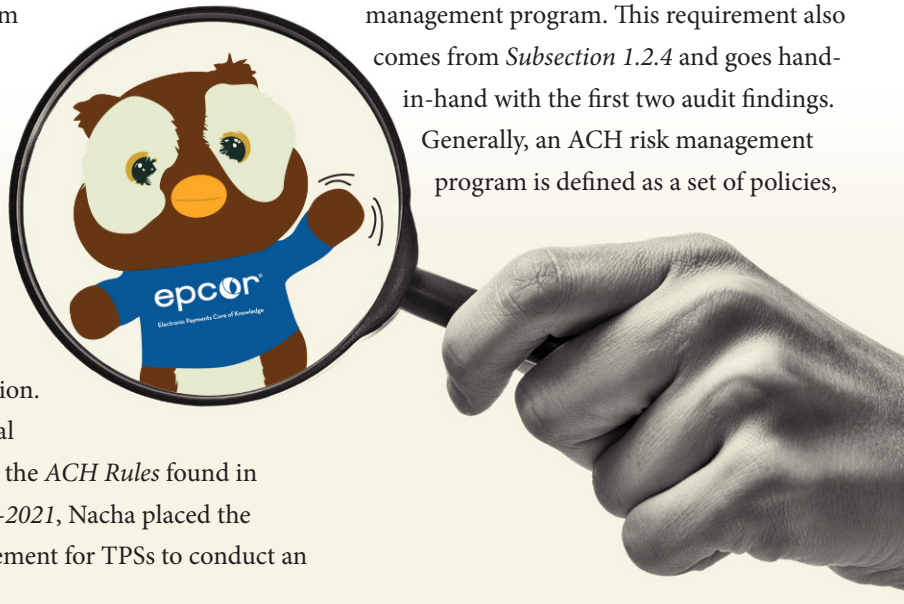
Per the *ACH Rules*, just like participating financial institutions, Third-Party Senders (TPS) are required to conduct an annual ACH Compliance Audit. The EPCOR Audit team performs TPS audits each year which often result in repeated findings and recommendations from one audit to the next. In this article, we will look at the audit issues we most often encountered throughout 2022, and the corresponding recommendations to assist TPSs in developing a strong ACH risk management program and promote ongoing *ACH Rules* compliance.

#1: Failure to Perform an ACH Audit

Easily, our number one audit finding was failure of the TPS to perform an ACH Compliance Audit each of the past six years. The *ACH Rules* require a TPS to have an ACH Compliance Audit conducted annually, and per *Subsection 1.2.2.2, Proof of Completion of Audit*, a TPS must retain proof of its annual audit for six years from completion of the audit. If the TPS was being audited for the first time in 2022 or had only begun its audit regiment a few years prior to 2022, the TPS was not able to exhibit proof of completion of prior audits for each of the past six years. EPCOR TPS audit reports remind the TPS to have the audit performed every year by December 31st, and to retain such documentation in accordance with *Subsection 1.2.2.2*.

#2 Failure to Conduct an ACH Risk Assessment

The second most frequent audit finding/recommendation was failure of the TPS to conduct an ACH risk assessment. Even before Nacha added TPSs to the risk assessment requirement in *Subsection 1.2.4, Risk Assessments*, EPCOR auditors had advised TPSs to perform an ACH risk assessment as part of creating an overall ACH risk management program for their organization. With the formal amendment to the *ACH Rules* found in *Supplement #3-2021*, Nacha placed the explicit requirement for TPSs to conduct an ACH risk assessment and added the effective date of September 30, 2022. During 2022, EPCOR noted that the majority of TPSs had not established an ACH risk assessment. The primary reason for this omission was lack of awareness of the requirement. However, a failure to understand the purpose of the risk assessment and/or its role in the overall ACH risk management program for the organization was also noted.



#3 Failure to Establish an ACH Risk Management Program

Another frequent audit finding was failure of the TPS to establish an ACH risk management program. This requirement also comes from *Subsection 1.2.4* and goes hand-in-hand with the first two audit findings. Generally, an ACH risk management program is defined as a set of policies,

procedures, limits, assessments, reviews (audits) and reporting protocols that govern the overall ACH activities of the TPS.

While TPSs have a large degree of flexibility in the composition of their ACH risk management program, general objectives of the program should include:

1. assessing the risks of the activity (risk assessment),
2. creating comprehensive know-your-customer (KYC) and onboarding due diligence (policies/procedures),
3. establishing controls over Originator and Nested TPS activity (limits),
4. setting up monitoring and reporting systems (reporting) and
5. providing for periodic audits.

Specifically, *Subsection 2.2.3, ODFI Risk Management* (which also applies to TPSs), requires the TPS to perform due diligence on each Originator (and Nested TPS), to assess the nature of the Originator or Nested TPS's ACH activity, implement and enforce exposure limits for each Originator or Nested TPS and monitor ACH Return activity. All these duties are to allow the TPS to determine that the Originator or Nested TPS has the capacity to perform its *ACH Rules* obligations.

#4 Failure to Maintain Proper Agreements

A fourth audit finding that was frequently noted is noncompliance with *Subsection 2.2.2.2, ODFI Must Enter Origination Agreement with TPS* of the *ACH Rules*. Specifically, it is *2.2.2.2(h)* and *(i)* that are of paramount importance to the TPS. Letters *(h)* and *(i)* of *Subsection 2.2.2.2* require the TPS to enter into ACH Origination Agreements with each Originator, or Nested TPS, respectively.

While audits almost always determine that TPSs have contractual agreements with the client Originators and/or Nested TPSs, what is often discovered is that the agreements fail to include the specific, minimum ACH provisions found in *Subsection 2.2.2.1*(a – f) of the *ACH Rules*. Nacha provides some leniency on this Rule in that old agreements without the required, minimum provisions are permitted to be carried forward. However, as agreements are revised or repapered, the TPS should ensure the agreement provisions detailed in *Subsection 2.2.2.1* are properly included. Such flexibility aside, it has been EPCOR's audit recommendation for the TPS to add the required provisions as soon as possible. We often suggest creating an "ACH Addendum" that can be added to the existing agreements without a complete repapering project.

Notable Mention Findings

Other less frequently cited audit findings still worth noting for TPSs include:

- failure to establish exposure limits,
- failure to act on Notifications of Change (NOCs),
- incorrect assignment of Standard Entry Class (SEC) Codes,
- inadequate authorization language,
- lack of monitoring of Originator Return Rates and
- best practice suggestions for the establishment of a formal ACH Management Policy and the establishment of procedures to acquire authorizations or other ACH-related documents from Originators and/or Nested TPSs.

If you're a TPS, I hope this article has been thought-provoking and opened your eyes to potential issues and areas to consider making changes to ensure you are compliant with the *ACH Rules*. Just remember your financial institution is your ally. If you feel like you need additional education or guidance from them, reach out and work together to come up with a solution that works for everyone.

EPCOR offers resources for Third-Party Senders to further develop your understanding of TPS *ACH Rules* requirements and beyond. If you're a TPS with questions, we encourage you to reach out via phone (800.500.0100), email (memserve@epcor.org) or chat with us on our website (epcor.org) and let us help guide your organization in the right direction! We would be happy to help you navigate your next steps from an educational or training perspective. We hope to hear from you soon!

Don't Fall Victim to Current Debit Card Fraud Trends

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

EPCOR's team has continuously heard tales about debit card theft and fraud. While creating duplicate cards is harder than ever, thanks to most cards having an EMV chip and many merchants installing EMV chip reading devices, debit card fraud is still an ongoing issue due to cards being stolen, devices being hacked or stolen and databases containing debit card information being breached.

Current fraud trends to watch:

- **Fraud at Retail Stores.** Financial institutions are seeing an increase in debit card theft happening at retail stores. For example, wallets are being stolen from purses while the cardholder is waiting in line at the checkout or while chatting with the cashier. Then, the thief takes the stolen debit card to another retailer to buy goods and makes the purchases on EMV-ready devices. A big issue here is you cannot charge the funds back to the merchant via the card network because they have EMV devices installed. This creates pain in the form of Reg E write-off losses when handling disputes because the stolen Debit Card led to unauthorized charges.
- **Social Scamming.** There are many scams where fraudsters reach out via phone calls, emails, social media and other available avenues to request an account holder's debit card number. Many account holders are receiving scam emails or phone calls from fraudsters posing as their own financial institutions. Please note:
  - ⇨ A person's debit card is theirs and theirs alone. The information should not be shared with anyone. Everyone should guard this information like you would your social security number.
  - ⇨ A financial institution will never directly request information such as a person's debit card numbers, as they already have that kind of account information on file.
  - ⇨ Account holders should never give out their login credentials to anyone for online banking systems or apps for any reason.
- **Fraud Using Digital Wallets**. This type of fraud appears to be on the rise, as fraudsters are stealing card info and then inserting said information into their own digital wallet, such as Apple Pay, Google Pay, Samsung Pay or their own financial institution. Then, they'll just tap their phone at a retailer that accepts Near Field Communication (NFC) based payments or use whatever apps accept digital wallet payments. As an FYI, when the phone is tapped at an NFC device, that is a "point of sale card present" payment whereas goods/services purchased from an app is considered "card not present".
- **ATM Skimmers.** There are still ATM skimmers out there, whether that is placing a device over the card reader or drilling holes in the ATM to insert a skimmer on the chipset. However, lately, fraudsters are getting even more clever and are creating devices small enough to be inserted into the card reader itself to steal information. Additionally, phony panels that look exactly like what is normally on an ATM are being inserted, and they have tiny pinhole cameras to watch for PIN entry. While skimming technology may be difficult to overcome, advising your clients to cover their hand while entering their PIN could help reduce the incidence of fraud on their card.

Here are a few additional debit card fraud prevention tips:

- Safeguard your debit card, smartphone and computers.
  - ⇨ Keep your cards and devices in safe locations and out of reach.
  - ⇨ Implement complex passwords/passcodes, both to unlock the device and to access accounts on Apps and websites.
- Anytime you can use Out-of-Band Authentication (OOBA) to verify any payments performed on apps or websites, the better.
- Always be careful where you swipe your card.
- Utilize online banking either in website form or your financial institution's app to check your online statement daily for any out-of-the-ordinary transactions. Make it a habit to check your account activity at least once daily and opt-in to receive alerts for account transactions.
- Look out for each other. If you see any friends, family, co-workers or even complete strangers appearing to fall victim to a scam, speak-up and say something if you feel comfortable doing so. Sharing information can help reduce the incidence of fraud.

Stay safe out there! And if you're looking for additional information on how you can avoid fraud, visit epcor.org/corporateuser for more corporate-focused fraud education and EPCOR's YouTube channel for short informational videos!

Fast, Faster or Instant: What's Your Payment Preference?

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

When it comes to making a payment, a payment is a payment is a payment, right? Yes, in the sense that a consumer or business intends to pay for goods or services. And while your financial institution likely offers a variety of options, how might your organization choose one payment means over another?

Perhaps one consideration is whether your organization wants to fund the purchase out of current income or with borrowed funds. Some other reasons may include ease of use, familiarity, convenience and cost. Or your organization may prefer to use a payment method that is safe and secure or universally accepted. However, in today's ever-changing (and rapidly) payments ecosystem, consumers and businesses may also make the decision based on how quickly the payment needs to be in the payee's account—fast, faster or instantly.

But what payment options are considered fast? Faster? Instant? Cash would be considered fast when compared to bartering as are checks, debit cards and next-day ACH. However, Same Day ACH and wire transfers fall into the faster category. And that leaves RTP® and FedNow℠, which are instant payments. While fast payment options are good and still serve a purpose, faster and instant payments are what many organizations are interested in these days. So, let's further define them!

Faster Payments

With faster payments, a payee's deposit account is credited or debited a few hours after a payment order has been initiated. Same Day ACH allows credit and debit payments to be originated, processed and settled all on the same day. Same Day ACH payments are accumulated throughout the day and then offset against each other, with only the net differential transferred between financial institutions (known as deferred net settlement). A wire transfer is also a faster payment; however, individual transactions settle as they are processed (known as real-time gross settlement). Both Same Day ACH and wires may only be processed during certain hours Monday through Friday, excluding federal holidays. This is one key feature that keeps them from being instant payments.

Instant Payments

With instant payments, clearing and settlement occur in real-time for each individual credit transaction, and funds can be sent and received around the clock, any day of the year. The transfer of funds between the payer and payee's accounts at financial institutions occurs within seconds and funds are final and irrevocable. RTP®, which was implemented November 2017, and FedNow℠, which goes live July 2023, are examples of instant payments.

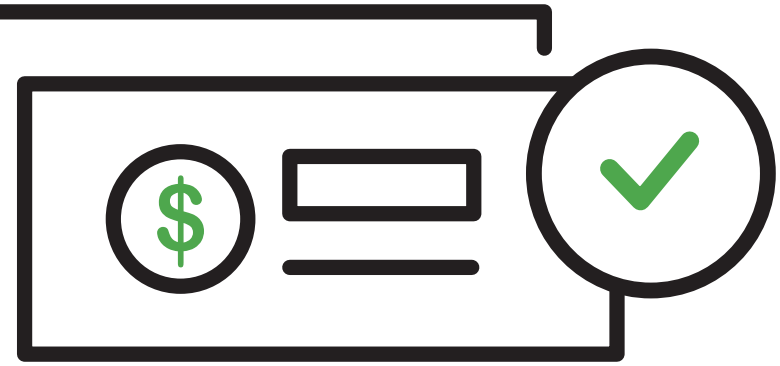
RTP® and FedNow℠ are different from ACH in the fact that the systems operate on a 24/7/365 basis. Gone are the constraints of normal banking hours. Along with a completely wide-open timeframe, RTP® currently can be, and FedNow℠ will be, utilized by consumers, businesses and financial institutions. Anyone anywhere can participate in instant payments (as long as they have connection to the given network). These benefits of speed, convenience and accessibility are what set RTP® and FedNow℠ apart from traditional payment methods.

Interested in utilizing some form of faster or instant payments at your organization? Reach out to your financial institution to learn more and discuss your options.

The Check's in the Mail... Or Is It?

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

How many of us have ever put an outgoing bill/invoice in our home/business mailbox or a blue U.S. Postal mailbox? It is true that Americans have decreased their use of check payments, however; cases of check fraud continue to soar. Criminals are targeting USPS blue collection boxes, unsecured residential mailboxes, privately owned cluster box units at apartment complexes and high-density commercial buildings to gain access to funds to perpetrate a scam.



After stealing checks from a mailbox, fraudsters will alter or "wash" the check, replacing the Payee name with a fraudulent consumer or business name and deposit the checks into fraudulent accounts they have set up. They often will wash and alter the amount of the check as well. Fraudsters have also gotten crafty at stealing business checks and creating authentic-looking counterfeit checks that are utilizing real account and routing numbers but are deposited using fake identities.

Why has this type of fraud become so profitable for fraudsters? Well, there are numerous ways checks may be deposited in today's environment that give immediate availability but have less monitoring, such as image-enabled ATMs and remote deposit capture.

What can consumers and businesses do to combat this type of fraud? Be vigilant in reviewing your transactions online with your financial institution daily if not more often.

Why is remaining vigilant so important? Financial institutions only have a 24-hour window to return a check after it has been posted to your account. That is a very quick turnaround. Outside of that timeframe, your financial institution may be able to deal directly with the depositing financial institution to try and recover funds for altered checks or forged endorsements. With the number of these claims flowing through the financial system today, it could take months up to a year to get the issue resolved, but it is not guaranteed that funds will be reimbursed.

Reviewing your transactions daily is imperative, especially if you are a business that has had your checks counterfeited. Again, your financial institution only has 24 hours from when the item posts to your account to get it returned. Your financial institution will have a timeframe specified within their deposit agreement of how long they give you to review your account statement and report that an item is altered or counterfeit. It is important that your business is aware of that timeframe, as the loss could fall on you if you don't notify your financial institution in a timely manner.

Another major issue that could impact your organization is when a check payment sent to you by your client is intercepted by a fraudster. This scam causes issues for the business and the consumer. The consumer believes they paid their bill/invoice on time, and the business is sending out late notices as they never received the payment. My advice to your business in this situation is to work with your consumer to resolve the error. The consumer will need to contact their financial institution and notify them that the check cleared their account but that the named Payee (your business) didn't receive the funds as intended. The financial institution will then need to file a claim to the depositing financial institution on the consumer's behalf, which often requires a written statement from your business stating you never received the funds.

The Financial Crimes Enforcement Network (FinCEN) issued an alert earlier this year to financial institutions with tips on how to detect, prevent and report suspicious activity associated with mail theft-related check fraud. Some of the red flags that financial institutions are looking for are:

1. Non-characteristic large check withdrawals on accounts with a new Payee.
2. Account holder claims a check they put in the mail was never received by the recipient, however; the check cleared their account.
3. Checks clearing on accounts appear to be a different color or not within the check range of other checks issued.
4. Account holders with no history of check deposits start experiencing large check deposits followed by a rapid withdrawal or transfer of funds.
5. Checks have appeared to have been washed using chemicals and Payee and/or amounts have been altered.

Combatting this type of fraud begins with account holders being diligent in reviewing their account history via their institution's online banking or utilizing a positive pay service that your institution may be offering to your business. If you have any questions about your responsibilities as an organization, contact your financial institution.

Sources: ABA, Sterling Compliance

epcor®

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
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665