CITIZENS STATE BANK
epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

The Best Defense Is a Good Offense

by Emily Nelson, AAP, APRP, NCP, Manager, Payments Education, EPCOR

The adage that "the best defense is a good offense" means being proactive rather than passive can give you an advantage over your opponent—whether with your competition or in processing ACH payments. That's right! Even when it comes to initiating ACH payments. So, what can your company do to protect itself from potential losses related to disputed ACH debit transactions? First...

Authorizations (refer to the *Nacha Operating Rules, Section 2.3*, for complete requirements based on the type of ACH debit your company is sending)

1. Obtain proper authorization from the consumer prior to debiting their account. You should ensure the terms of the authorization are clear and readily understandable by the consumer. This means they must know:
   - ⇨ Whether they are authorizing one payment, multiple payments or recurring payments (e.g., payment made on a monthly basis), and
   - ⇨ How to cancel their authorization (i.e., include specific instructions on how to do so, such as submitting a request in writing or requesting cancellation via a phone call).
2. Provide a copy of the authorization, either electronic or hard copy, to the consumer.
3. Retain the original or copy of the authorization (electronic or hard copy) for your records and ensure it is securely stored. The *ACH Rules* require your company to keep this for two years from the termination (e.g., the consumer is no longer a client or has fulfilled their financial obligation) or revocation of the authorization. As a best practice, you may consider keeping it longer.
4. Prepare to respond to requests from your financial institution for proof of authorization. The timeframe in which it must be provided to them should be outlined within your ACH Origination Agreement. If you cannot provide proof within the prescribed timeframe or not at all, you could be required to accept the return of the payment. This means you would give the consumer back the monies collected and potentially suffer a financial loss.

You've followed the authorization steps and transmitted your ACH debit file to your financial institution, which sent it into the ACH Network for processing to the consumer's account. Now what happens?

Understanding the Role of the Consumer's Financial Institution

The consumer's financial institution is

responsible for processing ACH payments to the account number in the ACH entry. This means if the account number exists and there are enough funds to cover the debit payment, then it will automatically be processed. And life is good! Or is it?

The consumer is responsible for reviewing their account activity and notifying their financial institution of any errors. If they notice a debit that (1) they did not authorize, (2) they had authorized but have since revoked or (3) they had authorized that was processed incorrectly, such as for the wrong amount, they should contact their institution.

If the consumer's notification is within 60 calendar days of when the debit posted to their account, their financial institution can return the payment on their behalf. This means no investigation is required to determine if the consumer's claim is valid or not. Instead, based on the consumer's signed and completed Written Statement of Unauthorized Debit (WSUD), they can return the payment to your company's financial institution. Upon receipt, your institution must accept the timely returned entry and may then charge it back to your account. Now what?

Handling Returned Payments

If you have a copy of the consumer's authorization related to the returned payment, you must resolve the dispute directly with the consumer. In addition to having a copy of the authorization, you may ask your financial institution to request a copy of the Written Statement of Unauthorized Debit (WSUD) from the consumer's institution.

A WSUD is a legal document instructing the consumer's institution to return the payment. It does not relieve the consumer of any financial obligation to your company. Therefore, you may choose to seek legal counsel to recover any losses associated with the return of the payment. Or, you could work out an alternate payment plan with the consumer. The decision is yours.

Requests for copies of WSUDs must be made within one year from receiving the returned entry. The consumer's financial institution has ten banking days, which equates to approximately two weeks, to provide the WSUD to your financial institution.

The ACH Management Policy for Third-Party Senders

by Amy Donaghue, AAP, APRP, NCP, Director, Advisory Services – Risk & Third-Party Services, EPCOR

A Third-Party Sender (TPS) has specific *ACH Rules* obligations, including the requirement to implement an ACH Risk Management Program. An effective ACH Risk Management Program typically begins with the development and implementation of a formal ACH policy demonstrating a TPS's understanding of its role in the ACH Network and the risks involved with its activities by addressing key *ACH Rules* obligations of the TPS. Additionally, this policy provides statements, rules or assertions that specify the expected behavior of an organization by defining roles and responsibilities of staff and departments as well as conditions and requirements for products, services and systems. Essentially, the policy communicates an organization's values, philosophies and culture as it relates to ACH origination.

Having addressed the reason for the policy, let's talk about the content of the policy. There is no specific content requirement for any given policy. However, there should be enough information contained in the policy to determine which departments or individuals play essential roles in the activities addressed. Most policies will contain some type of scope that defines what the policy is addressing, as well as a strategic objective of the goals a company is striving to achieve. The policy also provides insight into an organization's risk tolerance levels and helps to ensure staff understand their roles and responsibilities to meet the strategic goals of the organization in an acceptable manner. This is the reason the ACH policy is most often thought of as the cornerstone and formalization of a TPS's ACH Risk Management Program.

The structure and content of an ACH policy are driven primarily by the organization's ACH participant role, the type of clients it provides services to and the type of ACH entries that are being processed. If you were to review an ACH policy of a payroll services provider, it most likely would differ in content from that of a TPS providing check conversion services to clients. Policies could also contain information about other activities, such as the data security that has been implemented specific to ACH activities. Also, it may contain information specific to Customer Identification Program (CIP) and Know Your Customer (KYC) requirements. Again, defining the roles and responsibilities for each of these activities is critical.

Also, it is considered acceptable to reference other policies within the ACH policy. For instance, if there is already a robust, comprehensive AML Policy that addresses CIP, KYC and OFAC responsibilities, there is no need to restate that information in the ACH policy. However, it is recommended that the ACH policy clearly make the statement that those activities will be addressed in another specific policy. Such policies are traditionally thought of as requirements of a financial institution to have implemented. One of the key elements noted within the *ACH Rules* is that a TPS will take on the roles of an ODFI and becomes

subject to many of the same Rules and best practices, including the development of various policies and written procedures.

Additionally, policies are not meant to remain a static document that, once developed, approved and implemented, become just another document provided when requested. Policies should be reviewed at least annually to determine if they still contain relevant information of the TPS's processing environment. Policy changes should be documented to better determine when a new statement or requirement has been added. Updated policies should also be provided to any stakeholders that are subject to the requirements of the policy. Some organizations will also require staff to formally acknowledge the receipt and review of updated policies.

To assist TPSs, EPCOR has developed a new publication, the *Sample Third-Party Sender ACH Management Policy*. This sample policy covers *ACH Rules* and various other policy best practices impacting essential ACH processes such as ACH origination, Nested Third-Party Sender relationships, Originator strategies and onboarding requirements. Our team of experts is also prepared to help in any way we can! Reach out to EPCOR at advisoryservices@epcor.org to learn how we can help you enhance your TPS risk management practices.

Protecting Your Identity: A Crucial Guide to Safeguarding Your Personal Information

In today's digital age, where technology permeates nearly every aspect of our lives, the threat of identity theft looms larger than ever before. Did you know that more than 40 million U.S. consumers fell victim to some form of identity theft in 2021 alone?

Shockingly, according to Javelin's research, traditional identity fraud losses surged to a staggering $24 billion in 2021, marking a disturbing 79% increase over the previous year. When combined with losses from scams where individuals unwittingly provide personal information, the total losses soared to a staggering $52 billion.

Identity theft occurs when someone unlawfully uses your personally identifiable information (PII) for their own gain. This includes sensitive data such as social security numbers, credit card details and dates of birth. With our lives increasingly intertwined with the digital realm, protecting this information has never been more critical. Whether it's healthcare data, financial details or even the identities of our children; no one is immune to the risks posed by malicious actors lurking in the virtual shadows.

Understanding the various forms of identity theft is the first step towards safeguarding yourself and your loved ones. From medical and financial identity theft to the alarming rise of synthetic identity theft, where fraudsters create fictitious identities using fragments of real information, the threats are multifaceted and ever-evolving.

So, what can you do to minimize the risk of falling victim to these insidious crimes? Here are ten proactive measures you can take to fortify your defenses against identity theft:

1. **Utilize Strong Passwords:** Embrace the mantra of unique, complex passwords for each online account, and consider employing a password manager for added security.
2. **Exercise Caution with Public Wi-Fi:** Avoid accessing sensitive accounts over public networks, as they are prime hunting grounds for cybercriminals.
3. **Manage Bluetooth Usage:** Disable Bluetooth when not in use to prevent unauthorized access to your devices.
4. **Secure Your Mobile Devices:** Protect your smartphones with passwords or biometric authentication, and be mindful of the apps you install.
5. **Keep Software Updated:** Regularly update your devices' software and firmware to patch vulnerabilities exploited by cybercriminals.
6. **Monitor Financial Accounts:** Stay vigilant by reviewing your account statements regularly and setting up alerts for suspicious activity.
7. **Guard Your Mailbox:** Be mindful of the sensitive information that arrives in your physical mailbox and take steps to secure it, especially when traveling.
8. **Consider Freezing Your Credit:** Temporarily freeze your credit to prevent unauthorized access and regularly review your credit reports for any irregularities.
9. **Protect Your Social Security Number:** Safeguard this vital piece of information by limiting its exposure and verifying the legitimacy of requests for it.
10. **Safeguard Your Children's Information:** Shield your children from identity theft by securing their social security numbers and educating them about online safety.

While we cannot completely eradicate the threat of identity theft, staying informed and proactive can significantly reduce the risk. By implementing these measures and remaining vigilant, you can fortify your defenses against cyber threats and mitigate potential losses.

Stay safe, stay informed, and together, we can combat the scourge of identity theft in our increasingly interconnected world.

Did you spot the scams? If so, you're a total fraudbuster!

Test your knowledge by identifying if the following scenarios are fraud or legitimate.

Question 1: You receive an email from your financial institution asking you to log in urgently, as there was an unauthorized login on your account. The email contains a link to enter your credentials.

Answer: It's a scam. This email sounds pretty PHISHy to us! Your financial institution would never pressure you to sign in with a link.

Question 2: Someone calls you claiming to be from your financial institution. They say they need to discuss activity on your account, but first, they need your name, mailing address and account number to verify your identity.

Answer: We smell a scam! If you receive a call like this, hang up and call your financial institution. Be sure to look up a known phone number and not just redial the number who called you.

Question 3: A text comes through on your phone stating that your financial institution needs to verify your information or your account will be closed within 24 hours. Just click the provided link and log in, or you could face potential account termination.

Answer: Definitely a scam! Financial institutions rarely—if ever—send links via text, nor will they use scare tactics. To verify the message, call your local branch or the number on the back of your card.

Get tricked by one of the scenarios? Up your fraud-fighting knowledge by:

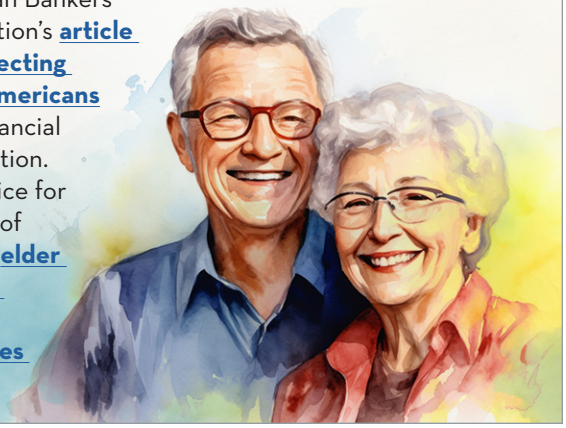
- **Visiting** BanksNeverAskThat.com and reading through their information and resources, taking quizzes, playing Scam City and more.
- **Watching EPCOR's fraud-fighting *Did You Know* videos**, available on YouTube, LinkedIn and EPCOR's website.
- Taking advantage of the Consumer Financial Protection Bureau's fraud and scam resources.
- Staying tuned to Fraud.org's fraud alerts.

Source: BanksNeverAskThat.com

Elder Financial Abuse Prevention

June is Elder Financial Abuse Awareness Month. Check out these resources to learn more about how you can protect vulnerable friends, loved ones and community members:

- EPCOR's ***Did You Know* video**.
- The Consumer Financial Protection Bureau's information on **reporting elder financial abuse**.
- American Bankers Association's **article on protecting older Americans** from financial exploitation.
- The Office for Victims of Crime's **elder fraud & abuse resources page**.



Don't Forget About Your Organization's Beneficial Ownership Information Requirements

FinCEN's purpose is to safeguard the financial system by identifying individuals involved in tax evasion, money laundering and even terrorist financing, and their most recent requirements largely impact small businesses by requiring them to file and report Beneficial Ownership Information (BOI). FinCEN began accepting reports on January 1, 2024. Many organizations will be required to report the required information by January 1, 2025. For additional information, **check out this article** from our previous issue of *Payments Insider* to better understand what's required of your organization. We also encourage you to visit FinCEN's **informational webpage** to learn more and file.

Understanding the 2024 *ACH Rules* Update for Corporate Originators and Third-Party Senders

In 2024, several significant amendments to the *ACH Rules* will take effect, impacting the way companies process ACH payments. It's essential for corporate Originators and Third-Party Senders to understand these changes to ensure compliance and efficiency in their payment processing operations.

Notifications of Change

One of the key updates impacts Notifications of Change (NOCs), effective starting June 21, 2024. Under this amendment, if the account information provided by a payee is erroneous or outdated, their financial institution may manually process the payment and send an NOC to the initiator. Corporate Originators need to update the information promptly for recurring payments and have discretion for one-time payments.

Prenotification Entries

Another significant change taking effect on June 21, 2024, is the expanded use of Prenotification Entries. Previously limited to verifying account validity before the first payment, this amendment allows companies to send prenotes at their discretion or as required by financial institutions.

Return Reason Codes

Return Reason Code updates take effect on October 1, 2024. This *Rule* change opens up Return Reason Code R17 to cover situations where the transaction is believed to be initiated under "false pretenses," addressing concerns related to fraud.

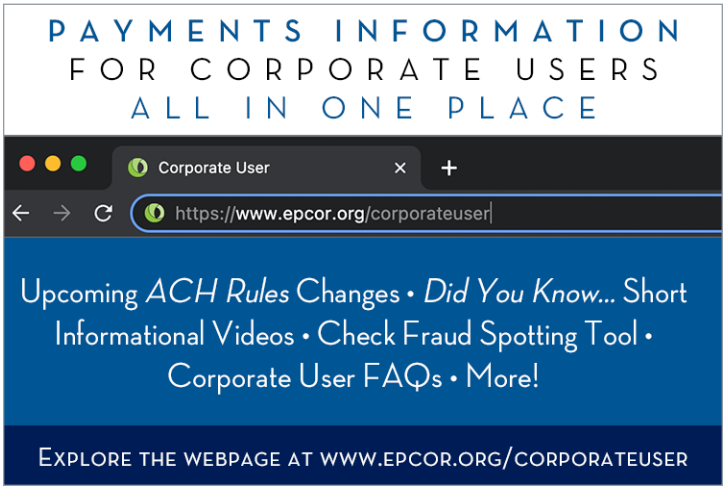
Similarly, Return Reason Code R06 will allow financial institutions to request returns for fraudulent payments. While this use case is not mandatory, this amendment provides a means for recovering funds lost to fraud.

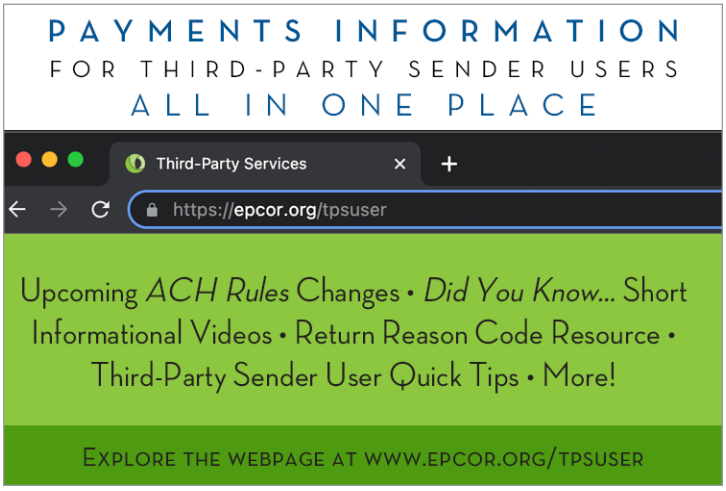
Other Rule Changes

Looking ahead to 2026, there are further changes regarding Standard Company Entry Descriptions and Origination Fraud Monitoring. The former outlines specific descriptions for payroll and online retail purchases, while the latter introduces requirements for companies to establish risk-based processes to identify and prevent unauthorized or fraudulent transactions.

In light of these updates, corporate Originators and Third-Party Senders must prepare by updating policies, procedures and systems to ensure compliance and mitigate fraud risks effectively.

For more information on these changes, download this *2024 ACH Rules Update for Corporate Originators and Third-Party Senders* document.





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.

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