INDIANA Members Credit Union
Keeping It Simple
epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

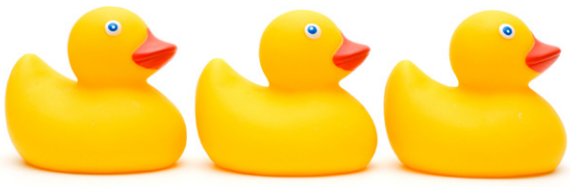
2022 *ACH Rules* Update for Corporate Originators

As an Originator of ACH entries, it is important to stay current with the *ACH Rules*, including how updates and changes might impact your business. Supplementing Data Security requirements and Micro-Entries are just a few of the changes on tap for 2022 and beyond. Get up-to-speed on these revisions and how they will affect your organization by downloading the ***2022 ACH Rules Update for Corporate Originators***. If you have any questions about how these changes may pertain to your existing Origination activities, contact your financial institution.

New Third-Party Sender ACH Rule: Time to Get Your Ducks in a Row

by Emily Nelson, AAP, NCP, Manager, Advisory Services, EPCOR

As the second quarter of 2022 kicks off, it is time to review plans to ensure upcoming requirements are being met. If you are a Third-Party Sender (TPS), then your plans should include preparation for Nacha's new TPS Rule.



Effective September 30, 2022, TPS roles and responsibilities under the *ACH Rules* will be updated. The purpose of the amendments made, as addressed on page ORxxxv, is to clarify existing practices surrounding Nested TPS relationships and make explicit the requirement for a TPS to conduct a risk assessment.

see DUCKS on page 2

Considerations for Accepting Cards and Cash Apps as a Small Business

by Allison A. Bramblett, AAP, Treasury Management Operations & Product Manager, The Farmers Bank

Card and digital payments have become a very popular payment method, and even more so over the last two years due to the pandemic. Digital payments are my go-to method when it comes to paying for my purchases; however, I have very recently started carrying a little bit of cash with me if I know I'll be shopping at any locally-owned shops or restaurants. Last year I found that a small mom-and-pop restaurant in my hometown started charging a 4% service fee if using a card to pay. I frequent this establishment to buy a Diet Coke® a few times a week and although 4% isn't a lot, it can add up over a period of time and

see APPS on page 3

DUCKS continued from page 1

Supplement #3-2021 does indicate that there will be a six-month grace period for certain aspects of each of the rules, but why wait? Let's highlight the areas to focus on and address now.

As a TPS, it will be necessary for you to identify any Nested TPS relationships for which you process ACH transactions. You will need to determine if the client you are processing for is processing on its own behalf, or on behalf of others whom the TPS has sold their services. If your client is processing on behalf of their clients, your client could qualify as a Nested TPS. You, the TPS with the direct relationship with the Originating Depository Financial Institution (ODFI), will want to ensure that you have an origination agreement in place with each Nested TPS and your Nested TPS has an agreement with their client. This reflects the requirements of *Subsection 2.2.2.2, ODFI Must Enter Origination Agreement with Third-Party Sender* and is an example of the "push down" effect for the chain of required agreements. As a best practice, it is recommended that these agreements are reviewed by your legal counsel.

If you identify Nested TPSs, it will be imperative that you make your ODFI aware immediately. Your ODFI will need to know how many Nested TPS relationships you are processing and will also need you to provide additional details regarding the Nested TPS's business information so updates can be made to Nacha's Risk Management Portal for TPSs. In addition, any time you are made aware of staffing changes within your organization or your Nested Third-Party's organization, you will need to provide the updated contact information to your ODFI in a timely manner so that your ODFI is able to update the registration information with Nacha within 45 days of the change, as prescribed in *Subsection 2.17.3.1, ODFIs with Third-Party Senders*.

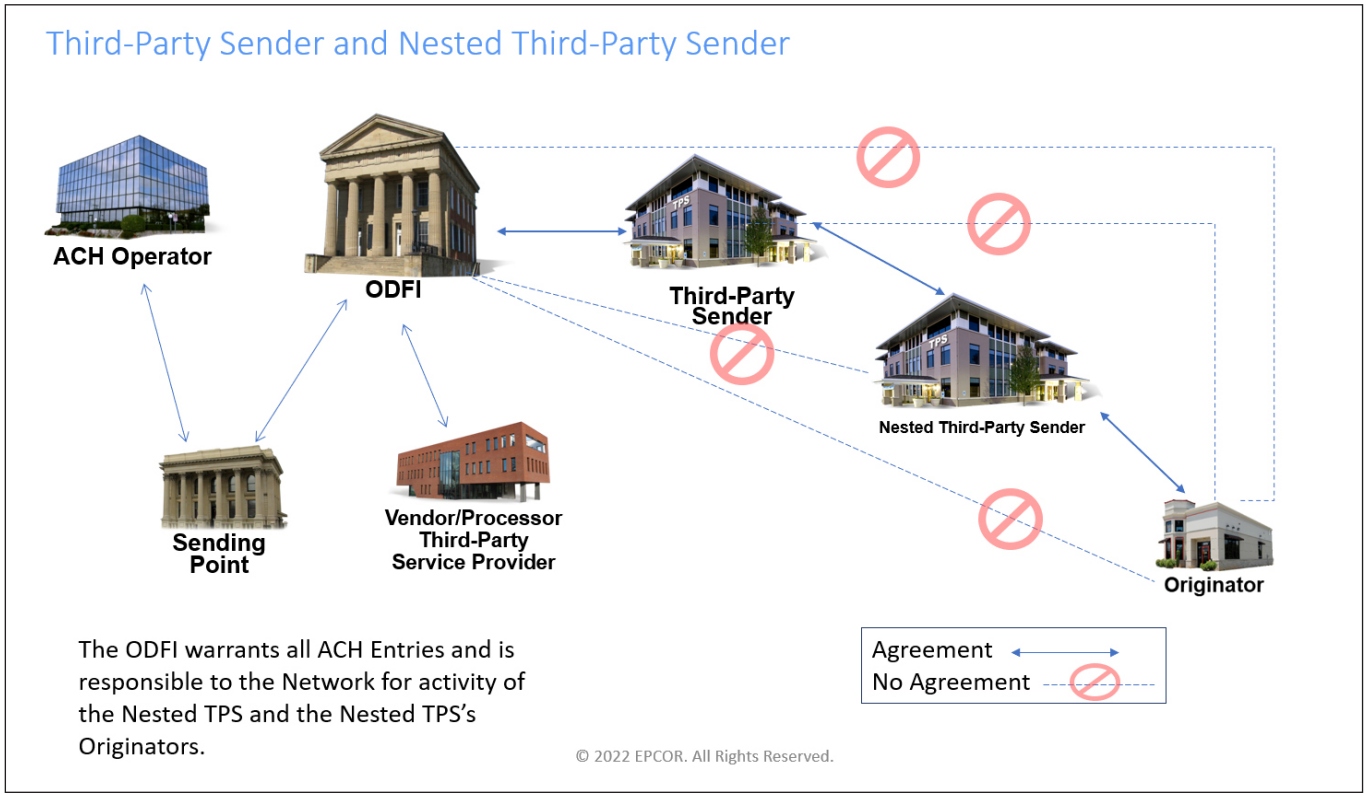
The updated application of the *ACH Rules* further dictates that Nested TPSs have an audit conducted annually, both TPSs and Nested TPSs have a risk assessment conducted and due diligence be conducted by the TPSs on their Nested TPSs. Also, Nested TPSs must conduct due diligence on their clients.

Additionally, all new *ACH Rules* will apply to TPSs and Nested TPSs. Annual ACH Rules Compliance Audits and periodic ACH Risk Assessments will need to be conducted by TPSs. TPSs will also need to ensure their Nested TPSs are aware of their audit and risk assessments obligations, as stated in *Supplement #3-2021*.

The ACH origination agreement between the TPS and the Nested TPS needs to address these obligations to protect both parties. As a TPS, you would want to ensure that your Nested TPS was able to attest to these items prior to transmitting any Entries.

These updates will largely impact TPSs and Nested TPSs but how these updates are handled by TPSs, in conjunction with their ODFI, will reflect in their successful transition for compliance.

If you have any questions, reach out to your financial institution.



APPS continued from page 1

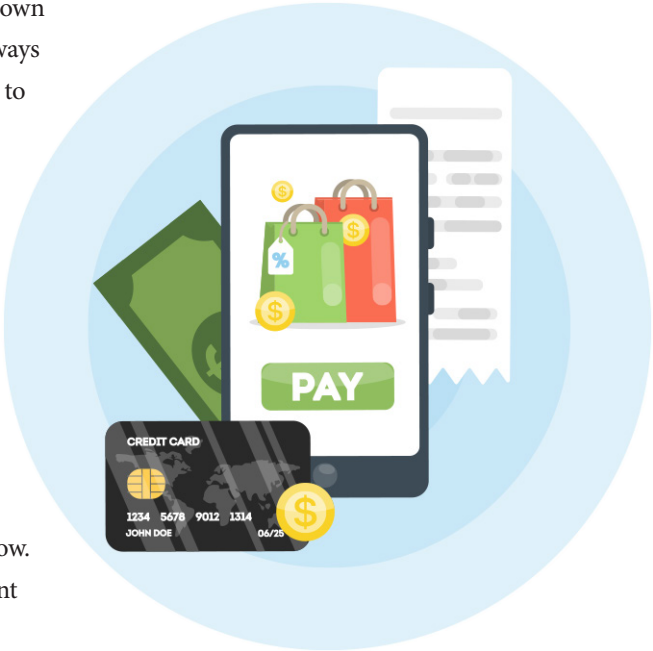
sometimes it's worth paying in cash to avoid any extra cost.

For those new to the card processing world, merchants (restaurants, retailers, storefronts, etc.) who accept cards must pay fees for each transaction they process, plus additional monthly fees depending on their processor, such as Square or Clover. Those transaction fees are typically assigned by the card brand (Visa, MasterCard, American Express or Discover®) and then partially switched around and given to the cardholder for rewards such as miles, cashback and points.

These fees eventually add up, and if you own and operate a small business it may not always make sense to offer a card payment option to your clients. My cousin and sister are both in the cosmetology business and I found my cousin, who owns the salon, didn't accept cards as a payment option until very recently. My sister has considered doing something to offset the cost of accepting cards as payment, but typically just increases her prices on an annual basis to offset any increase in general for service, product and card fees. She also accepts payment by Venmo, for now. Earlier this year a tax reporting requirement was put into place for businesses receiving more than $600 in payments for goods and services through payment networks such as Venmo, CashApp and PayPal. With this change, she, along with other self-employed individuals, are considering the pros and cons of accepting payments via an app.

So, what are some benefits to accepting cards or utilizing a payment app for your small business?

- **Increases Sales**—Giving consumers another option to pay when they don't have cash on hand allows your business to make a sale in situations where the client may have walked away if cards or payment apps were not accepted. Studies have shown cardholders tend to spend more when using plastic vs. cash.
- **Improves Cash Flow**—Funds are usually automatically deposited into your checking account within 1–2 business days. Additionally, this eliminates the timeframe of waiting for checks to clear, as well as the risk and liability of cash being stolen in the store and/or on the trip to your financial institution.
- **Broadens Business Model**—Adding the option of accepting card or payment apps could open the door for an online and social media presence offering goods and services for purchase through a website, resulting in more sales and income.



- **Convenience & Surcharge Fees**—Although business owners need to be careful on how and why they are charging fees for card payments, there are a couple of options to add a convenience fee or surcharge fee. There are rules and restrictions in place by each state and card brand, so businesses are encouraged to conduct research and due diligence prior to incorporating these fees. Adding these fees could help offset some of the costs incurred for offering to accept cards by passing them along to the cardholder.
- **Cash Discount Models**—For every transaction that is processed through the card network, there is a fee associated depending on the amount, card type, whether card is present, etc. This means if a debit card is used for an in-person transaction, the cost will be less than when a rewards business credit card is used online. For example, a debit card transaction may only cost 1.5% versus a rewards business credit card may cost 2.75%. Processors also have a way to implement a cash discount model for competitive pricing for card transactions. Therefore, it's important to do your due diligence when it comes to picking your processor and provider for your credit card processing. Processors like Square or QuickBooks® will charge a flat rate no matter the amount or card type, plus a per-item transaction. Payment apps will charge fees based on if the transaction is marked as a personal or a business transaction. Your best bet is to reach out to your local financial institution, because they likely offer this cash discount model type and want your business to succeed.
- **Convenience**—Most processors have made the set-up process very simple, enabling your business to begin accepting card payments within a short number of days. Payment apps have a similar simple setup and activation process. Once completed, you as the business owner and your clients will wonder why you hadn't added this convenient option a long time ago!

No matter what form of payments your business accepts, know there are always options to help reduce the cost of each payment method. Going through the pros and cons will help and if you still need guidance, don't hesitate to reach out to your financial institution.

Synthetic Identity Fraud: 5 Reasons to Stay Vigilant

The following information originally appeared on FedPaymentsImprovement.org.

In the continued progress toward a vision of faster, safer and more efficient payments in the United States, synthetic identity fraud is a high priority for the payments industry and broader U.S. economy. This fraud type is running rampant and impacting businesses across multiple segments. Here are five reasons you should stay vigilant:

- **Accounts for substantial financial loss**—Often miscategorized as a credit loss, synthetic identity fraud accounted for an estimated $20 billion in losses for U.S. financial institutions in 2020.
- **Growing in frequency and impact**—The ease of synthetic identity creation, combined with the increase in digital app capabilities, has simplified the process of creating these fictitious identities, allowing them to penetrate the financial system.
- **Often undetected by traditional fraud detection models**—Most traditional fraud detection models are not built around the concept that a person is not real.
- **Numerous avenues for fraud**—The same synthetic identity can be used to defraud multiple industries at the same time, including the financial industry, healthcare industry and government.
- **Potentially devastating impacts on individuals**—Although the initial financial impact is usually felt by a financial organization, the use of synthetic identities can also negatively affect individual consumers and companies.

The Federal Reserve recently released a Synthetic Identity Fraud Mitigation Toolkit to provide financial institutions, consumers and businesses with an online repository of insights and resources on synthetic identity fraud. The toolkit is designed to enable all payments participants to better identify and fight this fraud. The resources within the toolkit are downloadable and focus on the basics of synthetic identity fraud, how it's used, additional information on common use cases and tools to help identify and prevent this fraud.

To explore the toolkit, visit this link: https://bit.ly/idfraudtoolkit.

Want a quick tutorial on synthetic identity fraud? Check out EPCOR's *Did You Know* video, available on YouTube, LinkedIn and EPCOR's website. And be sure to check out the many other *Did You Know* videos on a variety of fraud and general payments topics. These videos are a great way to share important knowledge forward with your team members, clients and loved ones.

Source: FedPaymentsImprovement.org

Free Resources at Your Fingertips with EPCOR's Corporate User Webpage!

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

In 2021, with the help of our Cash and Treasury Management Committee, EPCOR designed a corporate user webpage filled with valuable resources and information for corporate users. This webpage is well maintained, and new resources are added continually.

On the webpage you'll have access to:

- EPCOR *Did You Know* videos
- Free webinar on ACH Security Framework for Originators
- Information on upcoming *ACH Rule* changes
- ACH FAQs
- The latest *Payments Insider* issue
- So much more!

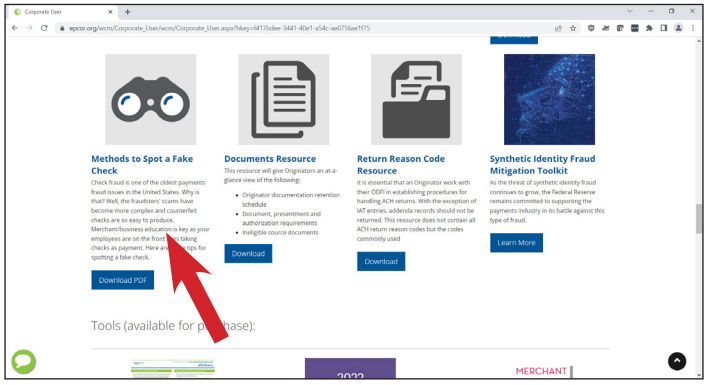
If you're wondering when this page would be helpful to you, check out these scenarios where the corporate user webpage provides necessary resources and information.

see RESOURCES on page 5

RESOURCES continued from page 4

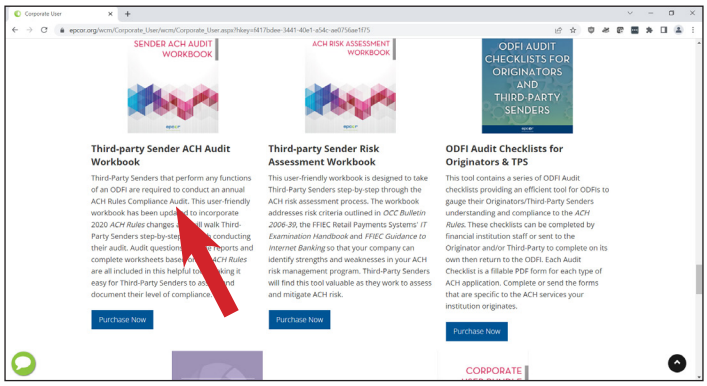
My company has been receiving lots of counterfeit checks lately. How can I determine if a check is counterfeit?

Check out our Methods to Spot a Fake Check PDF!



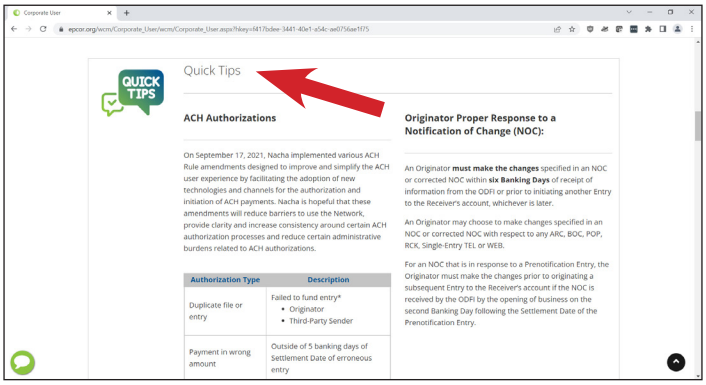
We are a Third-Party Sender and must conduct an ACH Audit and Risk Assessment annually.

Check out these helpful tools available to assist your organization.



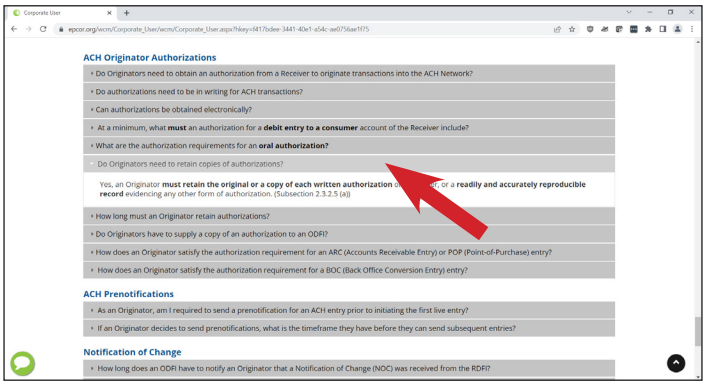
I am a new ACH Originator that just received a Notification of Change (NOC) from my financial institution. How many days do I have to correct the issue?

You must correct the issue within six banking days of receipt of NOC information or prior to initiating any other entries to the Receiver's account, whichever is later. This information (and more) can be found in the "Quick Tips" section on the webpage.



Must ACH Originators retain written authorizations?

Yes, Originators must retain the original or a copy of each written authorization or a readily and accurately reproducible record evidencing any other form of authorization. You can find this answer in the FAQ section of the webpage, along with the answers to many additional payments questions.



These are just a few examples of the resources and information available to you on the Corporate User Webpage. To access the webpage, visit epcor.org and select 'corporate user' in the toolbar.

Five Key Threats for Businesses and Consumers in 2022

The following article originally appeared on January 20, 2022, on BusinessWire.com.

Experian® recently released its annual *Future of Fraud Forecast*, which reveals five fraud threats for 2022. With consumers continuing to take a digital-first approach to everything from shopping, dating and investing, fraudsters are finding new and innovative ways to commit fraud. This year's threats include:

1. **Buy Now, Pay Never**—Recently, the Buy Now, Pay Later (BNPL) space has grown massively. In fact, the number of BNPL users in the U.S. has grown by more than 300% per year since 2018, reaching 45 million active users in 2021 who are spending more than $20.8 billion. Without the right identity verification and fraud mitigation tools in place, fraudsters will take advantage of some BNPL companies and consumers in 2022. Experian predicts BNPL lenders will see an uptick in two types of fraud: identity theft and synthetic identity fraud, when a fraudster uses a

see THREATS on page 6

THREATS continued from page 5

combination of real and fake information to create an entirely new identity. This could result in significant losses for BNPL lenders.

2. **Beware of Cryptocurrency Scams**—Digital currencies, such as cryptocurrency, have become more conventional and scammers have caught on quickly. According to the Federal Trade Commission (FTC), investment cryptocurrency scam reports have skyrocketed, with nearly 7,000 people reporting losses totaling more than $80 million from October 2020 to March 2021. In 2022, Experian predicts that fraudsters will set up cryptocurrency accounts to extract, store and funnel stolen funds, such as the billions of stimulus dollars that were swindled by fraudsters.
3. **Double the Trouble for Ransomware Attacks**—In the first six months of 2021, there was $590 million in ransomware-related activity, which exceeds the value of $416 million reported for the entirety of 2020 according to the U.S. Treasury's Financial Crimes Enforcement Network. Experian predicts that ransomware will be a significant fraud threat for companies in 2022 as fraudsters will look to not only ask for a hefty ransom to gain back control, but criminals will also steal data from the hacked company. This will not only result in companies losing sales due to the halt caused by the ransom attack, but it will also enable fraudsters to gain access and monetize stolen data such as employees' personal information, HR records and more—leaving the company's employees vulnerable to personal fraudulent attacks.
4. **Love, Actually?**—Because more consumers went on dating apps and social media to look for love during the pandemic, fraudsters saw an opportunity to create intimate, trusted relationships without the immediate need to meet in person. The FBI found that from January 1, 2021 – July 31, 2021, the FBI Internet Crime Complaint Center received over 1,800 complaints related to online romance scams, resulting in losses of approximately $133 million. Experian predicts that romance scams will continue to see an uptick as fraudsters take advantage of these relationships to ask for money or a "loan" to cover anything from travel costs to medical expenses.
5. **Digital Elder Abuse Will Rise**—According to Experian's latest *Global Insights Report*, there has been a 25% increase in online activity since the start of the pandemic as many, including the elderly, went online for everything from groceries to scheduling health care visits. This onslaught of digital newbies presents a new audience for fraudsters to attack. Experian predicts that consumers will get hit hard by fraudsters through social engineering (when a fraudster manipulates a person to divulge confidential or private information) and account takeover fraud (when a fraudster steals a username and password from one site to take over other accounts). This could result in billions of dollars of losses in 2022.

According to Juniper Research, merchant losses to online payment fraud will exceed $206 billion cumulatively for the period between 2021 and 2025. That's why it's crucial that businesses get the right fraud prevention tools in place to anticipate future scams and mitigate financial losses.

"Business and consumers need to be aware of the creativity and agility that fraudsters are using today, especially in our digital-first world," said Kathleen Peters, Chief Innovation Officer at Experian Decision Analytics in North America. "Experian continues to leverage data and advanced analytics to develop innovative solutions to help businesses prevent fraudulent behavior and protect consumers."

Looking for resources to fight fraud? Arm your staff and clients against common fraud schemes by sharing forward EPCOR's *Did You Know* videos, available on YouTube, LinkedIn and our website.

Attention Third-Party Senders! By September 30th, are you prepared to:

1. Identify Nested Third-Party Sender Relationships?
2. Update Processes, Procedures and Agreements Related to Third-Party Sender Relationships?
3. Ensure a Third-Party Sender ACH Risk Assessment is Conducted?

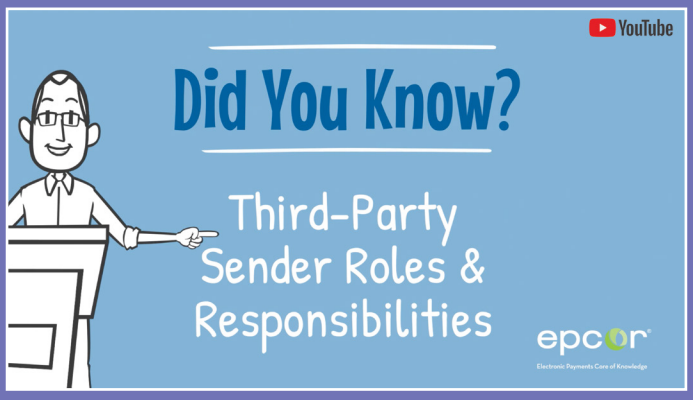
EPCOR Has the Resources You Need to Meet the New Requirements of Recent Third-Party Sender *ACH Rules* Changes

Resources for Third-Party Senders

- Third-Party Sender ACH Audit Services
- Third-Party Sender Risk Assessment Services
- Customizable Consulting Services for Third-Party Senders
- *Third-Party Sender ACH Audit* Workbook
- *Third-Party Sender Risk Assessment* Workbooks
- EPCOR Membership for Third-Party Senders

COMING SOON!

Visit epcor.org/thirdpartysender to explore these resources.



Watch our short *Did You Know* educational video explaining the changes available on YouTube (EPCORpymnts), LinkedIn (EPCOR – Electronic Payments Core of Knowledge) and epcor.org. Feel free to share it forward to clients and staff members.

INDIANA Members Credit Union

Keeping It Simple

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