epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

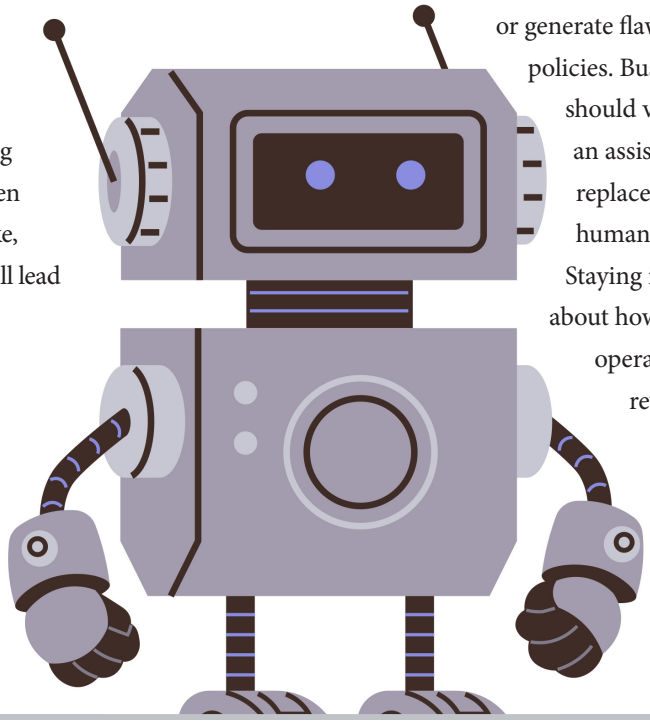
The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

Sleigh the Holiday Hustle with AI

by James Kallergis, AAP, APRP, Manager, Audit Services, EPCOR

If you've ever watched *The Terminator*, you know the fear—artificial intelligence (AI) taking over, humans sidelined… even in the bustling world of payments during the year-end rush. Using AI in business payments is a double-edged sword. It's hard not to see the advantages: AI can spot fraud faster than any human, simplify operations and even improve customer experience. But there's a catch—AI can also "hallucinate," producing results that appear accurate but are actually incorrect. And during this busy season, when fraud risks often spike, "almost right" can still lead to big problems.



Potential Benefits

For businesses that originate ACH transactions, AI can be a powerful tool. It can help streamline processes like payment reconciliation, spot unusual activity before it becomes fraud and even improve vendor management by recognizing transaction patterns. AI-driven customer service tools can also instantly answer common payment questions, freeing your team to focus on higher-value tasks.

AI's Shortcomings

Without the correct data or context, AI can easily misidentify potential fraud, suggest inaccurate payment actions or generate flawed internal policies. Businesses should view AI as an assistant, not a replacement for human judgment. Staying informed about how AI tools operate and reviewing their output critically is key to avoiding costly mistakes.

Turning the Tables on AI-Powered Fraud

AI isn't just in your hands; it's in the hands of criminals, too. Fraudsters are using tools like voice cloning to impersonate executives and trick staff into sending unauthorized payments. Synthetic identities can sneak through onboarding systems, and AI-generated phishing messages look more convincing than ever.

But AI can also help defend against these threats. Behavioral analytics can flag unusual transactions or login activity, and voice biometrics can detect cloned voices before fraud occurs. Still, these tools are only as strong as the humans overseeing them—someone must review alerts, validate findings and make informed decisions.

How AI May Fit into the New ACH Fraud Monitoring Rules

Beginning in 2026, new ACH fraud monitoring rules will require all Originators, Third-Party Senders and Third-Party Service Providers to have documented, risk-based processes to identify suspicious or unauthorized entries. For corporate Originators, that means taking a closer look at how your company monitors payments and vendor changes.

AI can be one option to help meet those expectations, but it's not the only way. Strong internal controls, manual reviews and traditional monitoring tools remain vital components of a solid fraud prevention strategy.

Why Human Oversight Still Matters

AI can process vast amounts of data and highlight patterns that might otherwise go unnoticed, but it lacks the intuition, judgment or accountability that human oversight provides. For business payments, context matters—whether it's understanding why a vendor's account information changed or whether an authorization really looks legitimate.

And at the end of the day, business is built on relationships. Your customers, vendors and employees still value human communication, especially when trust or money is at stake. Customers facing stressful situations don't want a chatbot. They want empathy, reassurance and clear answers from a real person. Empathy and understanding can't be automated.

"There is No Fate but What We Make"

AI is both a powerful ally and a potential liability. It can help streamline operations, strengthen fraud defenses and enhance customer service, but it can't replace human expertise or responsibility.

Like in *The Terminator*, the technology isn't inherently good or evil; it depends on who's using it and how. Businesses have the opportunity to harness AI thoughtfully, pairing innovation with accountability. The future of payments security and efficiency isn't predetermined, and this season of planning and preparation is the perfect moment to shape what comes next. As the movie reminds us: "*There is no fate but what we make.*"

'Tis the Season to Stay Fraud-Free

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

It's no surprise fraudsters made Santa's naughty list. The year-end rush means higher transaction volumes, more vendor payments and plenty of opportunities for criminals to slip scams through unnoticed. Your business could be at greater risk this season as employees make more purchases, approve last-minute invoices or send digital payments to partners and customers.

Help protect your organization from unwanted surprises—or lumps of coal—from landing on your year-end statements with these simple fraud prevention tips:

Check business accounts daily.

Monitoring transactions frequently helps spot fraud early, prevent further unauthorized activity and ensure issues are reported within required timeframes.

Set up account alerts and card controls.

Real-time notifications can flag unusual activity right away. Remind employees to review and update their alert preferences periodically to stay protected. Encourage cardholders to utilize expansive card controls (if offered) or protections in the form of limits, restrictions on merchants or types of transactions and locations.

Avoid mailing checks to vendors or partners.

Mail theft and check fraud increase significantly during the holidays, and stolen checks can be easily altered or counterfeited. Whenever possible, use secure electronic payment options, such as ACH, instead.

Keep company cards and devices secure while shopping or traveling.

This is a prime time for theft and skimming. Employees should safeguard corporate cards, avoid leaving personal belongings unattended and use trusted payment devices or networks.

Inspect card terminals before using them.

Fraudsters sometimes install skimming devices that steal card data and PINs. Before inserting or swiping a card, check for loose or suspicious parts. Tap-to-pay methods using tokenization offer safer alternatives.

Be cautious with online purchases or invoice payments.

Stick to verified websites and legitimate vendors. Fraudsters often mimic real businesses with fake domains or invoices, so always double-check payee information before approving a transaction.

Protect sensitive business information.

Never share payment or account details over unsolicited emails or calls. Remind staff that legitimate vendors or partners won't ask for confidential information they already have.

Verify recipients before sending digital payments.

Always confirm payment requests through a known and trusted contact or a verified phone number. Fraudsters are increasingly using fake payment accounts or AI-generated messages to create a sense of urgency and trick employees into sending funds.

Watch for business email compromise and phishing scams.

Cybercriminals frequently impersonate executives, vendors or IT support during the busy season. When in doubt, stop, think and verify (just like EPCOR's *Did You Know* video says) before sending payments or clicking links. For ACH, accepting account information by email is contrary to secure/encrypted transmission standards in *Section 1.7* and applicable legal requirements for credit authorizations in *Subsection 2.3.2.1* of the *ACH Rules*.

Watch for atypical origination requests versus recurring previous history.

Most ACH and wire transfer originations are sent repeatedly to the same Receivers, whether employees, vendors, utilities or lenders. Both originators and financial institutions should perform extra due diligence on payments sent to a brand-new Receiver or to an existing Receiver who suddenly updates their account information.

Utilize dual control for originated digital payments.

It's easier for a fraudster to compromise a single person than two. With dual control, one team member enters or uploads the payment while a second reviews it. The reviewer should carefully verify any new routing numbers or account combinations and question the source whenever something seems unusual.

If it sounds too good to be true, it probably is—especially with investment or crypto.

According to the FBI's 2024 IC3 Report, known investment scams resulted in over $6.5 billion in losses, while cryptocurrency-related scams caused more than $9.2 billion in losses. Fraudsters are becoming increasingly sophisticated, often impersonating trusted sources to target victims. Many schemes aim to drain long-term savings, Home Equity Lines of Credit (HELOCs), personal investments and 401(k) accounts.

While the holiday season can be hectic, your organization must remain vigilant with how payment information is used and shared. Encourage your team to stop, think and verify before approving payments or disclosing sensitive data. A few extra moments of caution can prevent significant losses and keep fraudsters exactly where they belong: on the naughty list.

Kick Off Your Payments New Year's Resolution

by Matthew Wade, AAP, AFPP, APRP, CPA, Senior Manager, Advisory Services, EPCOR

Ring in 2026 by giving your organization's payments strategy a fresh start. New opportunities and rules are on the horizon, and setting a payments-focused resolution now helps your business stay audit-ready, compliant and ahead of industry changes.

Audit-Readiness and Third-Party Oversight

Corporate Originators should be aware that automated proof of audit requests from Nacha are now sent directly to financial institutions. To stay compliant and reduce risk, complete your annual ACH audits. Reviewing full audit reports (not just confirmations) helps identify exceptions, verify compliance and address potential risks before they affect operations. Additionally, it's critical to regularly review company user permissions—removing access for employees who have left or changed roles—to prevent unauthorized access and reduce operational and compliance risks.

Regulation and Fraud Prevention

Regulatory changes, including Nacha's upcoming ACH fraud monitoring rules, are more than compliance checkboxes—they're essential to safeguarding your organization. Update internal controls, verify vendor and partner payments carefully and establish risk-based monitoring processes. Strong fraud defenses protect your company and maintain trust with partners and customers. For practical, step-by-step guidance, watch EPCOR's *Did You Know* video on the upcoming ACH fraud monitoring rules to see exactly how to prepare your organization.

Modernizing Payments Operations

The digital-first era and new payment rails, such as RTP® or the FedNow® Service, are redefining what's possible. Instant payments, artificial intelligence (AI), cloud computing and secure digital tools can help streamline operations, improve transaction speed and strengthen fraud detection. Exploring instant payment use cases with your financial institution can enhance liquidity and efficiency.

Enhancing Vendor and Customer Experience

Customers and vendors expect fast, secure and seamless payments. Leveraging modern technology and digital tools not only speeds up reconciliation but also builds stronger relationships. Personalization, frictionless approvals and proactive communication are key to maintaining satisfaction and trust.

When developing a payments strategy for your organization, consider these steps:

- Third-Party Senders should review their audits and examine reports for any exceptions or risks.
- Update processes and internal controls to comply with 2026 ACH fraud monitoring rules.
- Explore instant payment options such as RTP® or the FedNow® Service with your financial institution to optimize operations.
- Leverage AI and digital tools for efficiency but keep human oversight central to decision-making.
- Focus on vendor and customer experience to strengthen relationships while mitigating risk.

The road to a successful 2026 starts now. With audit readiness, compliance and modernization in sync, your organization can stride into the new year prepared for a smarter, safer and more efficient payments future.

SLEIGH Year-End Prep with Payments Resources

by Keldon Bowling,
Communications Specialist, EPCOR

Snow is gently falling, candy canes are lining the halls and the aroma of gingerbread fills the air—yes, the holiday season is officially here! As budgets get wrapped up like presents and goals are set under the sparkle of festive lights, it's the perfect time to prepare your team for the year ahead and set them up for success. If you have experienced staff nearing retirement, now is your organization's chance to train newer team members to step confidently into their roles. The best way to glide into 2026? Arming your team with knowledge and tools that make every payments process feel like holiday magic.

So, grab your peppermint cocoa, pull on your coziest sweater and get ready to SLEIGH your year-end prep by unwrapping the season's most wonderful gift: payments education for your team and clients!

ACH Rules

Staying compliant starts with easy access to the *ACH Rules*. If you don't have a copy or need extras, contact your financial institution to see if they can make a copy or additional copies available to your organization.

ACH Quick Reference Guide for Corporate Users

EPCOR's *Guide* provides a concise overview of the key *ACH Rules* every ACH Originator should know. It covers general rules, ODFI/Originator responsibilities, prerequisites, warranties and walks through essential processes such as returns, NOCs, prenotes and more.

Did You Know... Informational Videos

EPCOR's short, animated videos make complex payments topics easy to understand in just a few minutes. Perfect for sharing with team members or clients, recent videos include *New Fraud Monitoring Rules for ACH Originators*, *Stop. Secure. Report.*, *Stop. Think. Verify.*, *ACH Notifications of Change* and more. EPCOR also offers a business-focused series to help small businesses stay vigilant, covering invoice fraud, CEO impersonation scams, point-of-sale (POS) fraud prevention and more. Watch these videos on EPCOR's website, LinkedIn or YouTube channel.

Payments Insider

Payments Insider (which you're reading now) is a quarterly e-newsletter designed to keep organizations of all sizes up to speed on the latest payment system developments. The most recent edition is always available on EPCOR's Corporate User webpage.

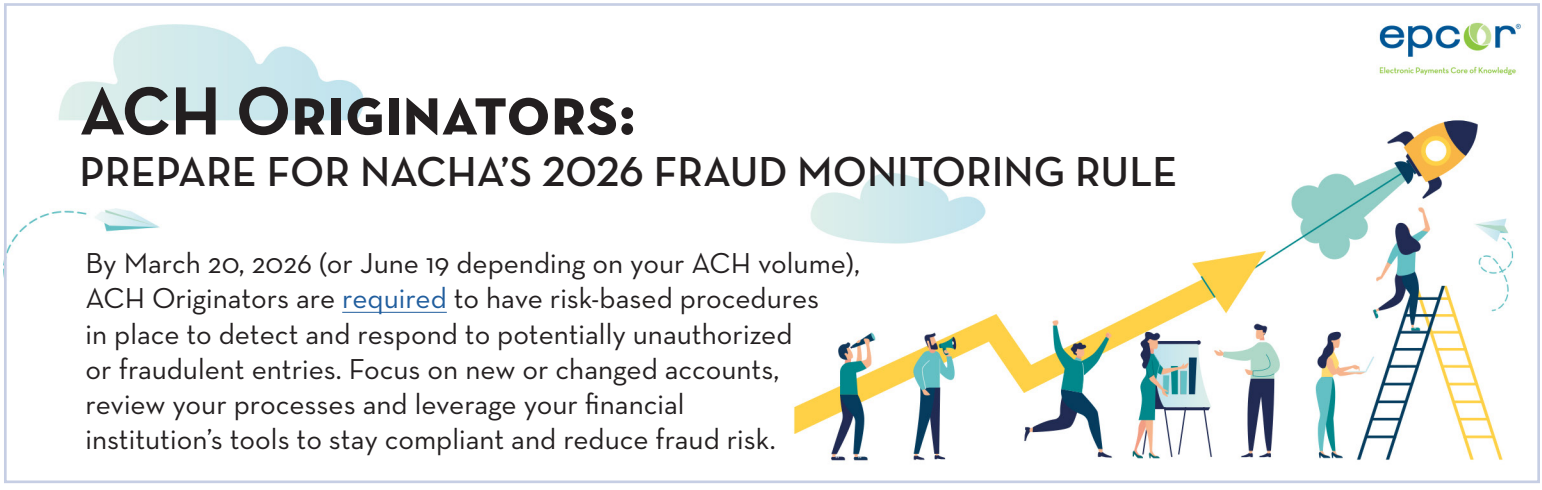
Corporate User Webpage

EPCOR's Corporate User webpage provides a variety of resources for end-users, including updates on upcoming *ACH Rules* changes and much more. The page is regularly refreshed with new materials, and visitors' suggestions are always welcome. Explore the resources by visiting epcor.org/corporateuser.

Third-Party Sender Webpage

EPCOR's Third-Party Sender webpage offers a range of resources, including sample agreements, helpful tools, educational videos, links to useful workbooks and more. Explore the page at epcor.org/tpsuser, and for any questions or guidance in finding the right resources, be sure to reach out to your financial institution.

As you prepare for the year ahead, don't hesitate to reach out to your financial institution for guidance or additional educational resources your team might need. Staying informed, asking questions and leveraging available tools ensures your organization can confidently navigate 2026 with efficiency, compliance and peace of mind. May your holidays be full of warmth, laughter and seamless payments!



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