THE KILLBUCK SAVINGS BANK CO. FDIC
epcor Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

How ACH Originators and Third-Party Senders Can Stay Audit Ready All Year..... pg. 1
The Trust Trap: The Hidden Objective Behind Bank Impersonation Fraud..... pg. 2
They're Gone. Their Payment Access Isn't: The Hidden Risks of Treasury Management Offboarding.... pg. 3
Commercial Insights: Payments News Bites for Small Businesses..... pg. 5

How ACH Originators and Third-Party Senders Can Stay Audit Ready All Year

by Liz Cone, AAP, AFPP, APRP, Director, FI Payments, Risk & Compliance, EPCOR



The ACH Network makes it easier for businesses to move money, but sending ACH Entries also comes with responsibilities. ACH Originators are businesses that send ACH Entries, such as payroll or payments, while Third-Party Senders (TPSs) provide ACH processing or payment services to Originators. If your business sends ACH payments or helps other businesses send them, you may be an Originator or TPS.

Staying organized throughout the year can help your business respond quickly when your financial institution or TPS requests documentation or reviews your ACH activity.

Know Your Role

For ACH Originators, consider these practical steps:

- **Keep authorization records:** Maintain evidence that customers or employees authorized ACH Entries and that changes or revocations are handled appropriately.
- **Use ACH correctly:** Make sure you use the appropriate Standard Entry Class (SEC) Codes and follow the terms of your ACH agreement.
- **Monitor your activity:** Keep an eye on transaction volumes, dollar amounts, exposure limits and Return activity. Investigate unusual activity or increases in Returns.
- **Keep records current:** Maintain current agreements, procedures, authorization records, training records and documentation showing how ACH issues were resolved.

For Third-Party Senders, consider these practical steps:

- **Know the businesses you serve:** Perform appropriate onboarding and due diligence before allowing an Originator or downstream customer to originate ACH Entries.
- **Understand their activity:** Confirm the purpose of their ACH activity,

expected volumes and dollar amounts, permitted SEC Codes and applicable exposure limits.

- **Monitor relationships:** Periodically review Originator and downstream customer activity, Return Rates, risk changes and compliance with agreements.
- **Keep evidence:** Document due diligence, reviews, approvals, issues and corrective actions so you can demonstrate that oversight is happening.

Make Audit Readiness Part of the Routine

You don't need to wait for an annual audit to check your ACH program. Set aside a little time each month or quarter to:

- Review a sample of authorization records.
- Confirm agreements and Originator or downstream customer information are current.
- Review Return activity and investigate exceptions.
- Check exposure limits against actual activity.
- Make sure issues have an owner, a due date and a documented resolution.
- Save supporting documentation as decisions and reviews happen rather than trying to recreate them later.

The goal is simple: If someone asked you tomorrow to show how your ACH program operates, could you quickly provide the records to support it? A little ongoing review can make that answer much easier.

The Trust Trap: The Hidden Objective Behind Bank Impersonation Fraud

by Art Moore, AAP, Director of Banking Operations, SVP, NBKC Bank

Bank impersonation fraud has evolved beyond phishing emails and fraudulent payment requests. Today's fraudsters are increasingly targeting the people who manage online banking and treasury systems, using sophisticated social engineering to make fraudulent requests appear legitimate and persuade trusted employees to take action.

While these attacks may appear focused on getting someone to send a fraudulent payment, the true objective can be gaining access to the systems businesses use to manage payments, users and account access. Criminals may seek to gain control of the treasury environment, enabling them to create users, modify permissions, redirect notifications and establish persistent access before ultimately executing fraudulent transactions.

As a result, fraud prevention is about more than protecting individual transactions. It also means protecting the access, administration and controls behind those transactions.

The Call That Looks Legitimate

Imagine you receive a text alert about suspicious activity on one of your business accounts. Shortly afterward, you get a call from someone claiming to be with your financial institution's fraud department. The caller appears knowledgeable, professional and concerned about protecting the account.

Everything feels legitimate, except it isn't.

Modern bank impersonation fraud relies on social engineering rather than technical compromise. Whether delivered through phone calls, texts, emails or spoofed websites, these attacks are designed to exploit trust and persuade victims to grant access or disclose authentication information.

Why These Attacks Work

Fraudsters often use urgency, authority and fear to convince their targets to act quickly. Common tactics include:

- Claims of suspicious account activity,
- Alerts about unauthorized login attempts,
- Warnings about compromised credentials or
- Claims of pending wire transfers requiring immediate action.

The deception can become even more convincing when criminals coordinate messages across multiple channels. Combined with caller ID spoofing and publicly available company information, it can be difficult to distinguish a legitimate financial institution representative from a fraudster.

The goal is often to get the victim to provide information or take an action that gives the fraudster access to the payment environment.

Why Payment Access Is So Valuable to Fraudsters

The online banking administrators at many businesses have access to a wide range of payment and account controls. They may manage wire transfers, ACH activity, online banking access, user administration and payment approvals.

That combination makes administrative access particularly valuable.

Fraudsters increasingly recognize that the greatest value may not be a single payment. It may be gaining control of the systems and permissions that enable future payments.

The Real Objective: Control the Environment

Once fraudsters obtain credentials, multi-factor authentication (MFA) codes or other access, they may attempt to make changes that allow them to operate within the payment environment.

Depending on the access they obtain, criminals may:

- Create users,
- Elevate permissions,
- Alter approval workflows,
- Register new devices,
- Add payees,
- Modify notification settings and
- Initiate transactions.

The fraudulent payment is often the final step; control is the primary objective.

For a business, the warning signs may not always look like a fraudulent payment. They could be a new user no one recognizes, an unexpected change to someone's permissions, a newly registered device or an alert that suddenly stops arriving.

Two Critical Post-Compromise Risks

Creating New Users: If a fraudster gains access to an account with user-management capabilities, they may be able to create additional user profiles, providing persistence and reducing dependence on the originally compromised credentials. These accounts can remain available for future fraudulent activity even after the initial compromise is discovered.

Redirecting Notifications: Many organizations depend on alerts for new users, entitlement changes, payment activity and security events. If criminals redirect or disable notifications, they can extend the time they remain undetected.

Together, these capabilities can give fraudsters a way to maintain access while making their activity more difficult to identify.

Protecting the Access Behind the Payment

Protecting the payment environment starts with protecting the access and controls behind it. Consider these practices:

1. Treat credentials, MFA devices and administrative privileges as high-value assets.
2. Monitor user creation, entitlement changes, device enrollments and administrative modifications.
3. Review changes to notification settings and alert recipients.
4. Independently verify requests involving access, credentials or authentication.
5. Regularly review users, permissions, approval workflows and registered devices.

It can also help to ensure employees know how legitimate representatives from their financial institution will communicate with them. Establishing verification procedures in advance can make it easier to slow down a suspicious request when urgency and pressure are being used to influence a decision.

Final Thoughts

The greatest threat posed by modern bank impersonation fraud is often not the unauthorized transaction; it is the unauthorized control that occurs first.

In today's threat environment, transaction verification alone is no longer enough. Organizations must also verify who controls the profiles, permissions and systems behind those transactions. Protecting payments is critical, but protecting control is just as vital.

They're Gone. Their Payment Access Isn't: The Hidden Risks of Treasury Management Offboarding

by Laura Zigler, AAP, Director of Treasury & Digital Banking, SVP, Mabrey Bank

When an employee leaves, most organizations have a well-established offboarding process. HR handles the paperwork, IT shuts down email and network access and equipment is returned. But one area can easily fall through the cracks: payment access.

An employee may no longer have access to their company email, but could still have permissions tied to ACH origination, wire transfers, corporate cards, check signing, instant payments or a treasury management platform. In today's increasingly connected payments environment, removing a network login doesn't necessarily remove the ability to move money.

Below are some steps to consider when removing an employee's payment access.

1. Start With a Complete Inventory of Payment Access

The first step is knowing where the employee has access. Don't limit the review to the primary online banking platform. Look across every payment channel the employee may have used, including ACH, wires, checks, cards and instant payments.

For example, an employee who served as a company's controller might have been an ACH originator and wire approver, an authorized check signer and a corporate cardholder. Each of those permissions may be managed in a different system or by a different department.

A good offboarding process should identify what the employee could do, not simply which systems they could log into.

Make sure to verify with your financial institution whether the employee had any personal devices registered as a trusted device for business banking.

2. Review Permissions, Not Just Usernames

Once access has been identified, review the employee's actual entitlements. Could they initiate an ACH file? Approve a wire? Issue and/or approve checks? Create bill payments? Add a new beneficiary? Release an instant payment? Manage other users?

This distinction matters because payment permissions can be more granular than a basic login. In some cases, an employee may retain a specific approval or administrative capability even after other access has been removed.



It's also worth reviewing payment limits and approval roles. If a departing employee was one of two people required to approve wire or ACH transactions, for example, the organization needs to ensure the remaining workflow continues to function and maintain appropriate separation of duties.

If the employee has payment entitlements, you may also need to review pending and scheduled transactions. Consider whether any transactions should be canceled or reapproved by another authorized employee. These transactions could include pending ACH/wire transfers, vendor payments, payroll files, recurring payments, future-dated transactions or transactions awaiting approval.

Depending on the circumstances of the departure, consider reviewing recent transaction activity for unusual activity, particularly around large ACH transactions, wires, internal transfers, new payees, changes to vendor information, changes to employee direct deposit information, linking new external accounts, unusual check activity and any transactions occurring immediately before termination.

3. Don't Overlook Cards, Checks and Other Physical Access

Digital payments tend to get most of the attention, but traditional payment methods deserve a place on the checklist.

Corporate cards should be deactivated or reassigned as appropriate, including virtual cards and access to expense-management systems. For checks, confirm whether the employee remains an authorized signer and whether any related Positive Pay or account permissions need updating.

These may seem like straightforward administrative tasks, but they are easy to miss when different payment channels are managed by different teams.

4. Pay Particular Attention to Instant Payments

Instant payments add another reason to make access reviews timely. With services such as the RTP® Network, the FedNow® Service and Zelle® for business payments, transactions can be initiated and settled around the clock, so an employee's payment authority shouldn't remain active simply because the departure occurred outside normal business hours.

As your organization expands its use of instant payments, make sure those permissions are incorporated into the same offboarding process used for ACH and wire access. The goal isn't to create a separate process for each new payment rail; it's to have a single comprehensive access-management process that covers all rails.

5. Review Administrators and Delegated Access

Some of the most important access isn't tied to someone who routinely initiates payments. An employee may be a treasury management administrator, backup approver or delegated user with the ability to change other users' permissions.

These roles deserve particular attention. A departing employee who can add users, change limits or modify entitlements may represent a very different risk than someone who can only view account information.

The same principle applies to third parties. Payroll providers, accountants, bookkeepers and other service providers may have payment access that needs to be reviewed when responsibilities or relationships change.

6. Use Offboarding as an Opportunity to Clean House

An employee departure can also be a useful trigger for a broader access review.

Maybe the company has grown since its treasury services were originally established.

Maybe an employee who once needed broad access now only needs one payment channel. Or perhaps several people have administrator privileges even though only one actually needs them.

Rather than simply replacing the departing employee's access, take a few minutes to ask whether the overall structure still makes sense. Consider reviewing dual control, approval limits, alerts and other payment controls while you're already evaluating user access.

Also review the employee's access to information, credentials and authentication methods that may be shared with other employees. For example, if Sally leaves but Joe remains an authorized user, Sally may have previously known Joe's credentials, had access to a shared email inbox or used a shared token.

The company should ensure that each remaining user has their own credentials and authentication method and that shared credentials are eliminated where possible.

Make Payment Access Part of the Offboarding Checklist

Offboarding shouldn't end when an employee's email account is disabled. For organizations that move money across multiple payment channels, it should include a review of every place that an employee could initiate, approve, modify or influence a payment.

ACH, wires, checks, cards, bill payments and instant payments may operate differently, but they share one important characteristic: they depend on the right people having the right access.

A consistent, cross-channel offboarding process can help your organization reduce payment risk, maintain appropriate separation of duties and ensure payment access stays aligned with employees' current responsibilities.

Commercial Insights: Payments News Bites for Small Businesses

For small business owners, keeping pace with how customers pay and how much those transactions cost is vital to maintaining healthy margins and smooth operations.

This quarterly briefing outlines the top five recent developments that directly impact your payment processing, cash flow and client experience.

1. Credit Spending Outpaces Debit

Recent industry data shows credit card usage is growing faster than debit card volume for the first time in nearly a decade. While higher credit spending often means larger average ticket sizes for your business, it also means higher average processing fees. Merchants should regularly audit their sales data to understand how this shift toward credit cards is impacting their bottom-line transaction costs.

2. The Battle Over Swipe Fees Moves to Court

Interchange and processing fees remain one of the largest operating expenses for



small businesses. Federal appeals courts are prepared to rule this autumn on proposed regulatory caps aimed at slashing debit card swipe fees by up to 28%. A favorable ruling will offer significant cost relief to businesses handling a high volume of everyday debit transactions.

3. Total Acceptance of Mobile Wallets

The retail landscape has hit a tipping point where contactless payments are no longer optional. With major nationwide retail holdouts officially adopting Apple Pay and Google Pay this past quarter, customer expectations for a unified, contactless checkout have reached an all-time high. Ensuring your checkout terminal or online gateway seamlessly supports mobile wallets is now mandatory to prevent cart abandonment.

4. AI-Driven Fraud Defense at the Point of Sale

Card networks have dramatically accelerated the rollout of predictive, AI-driven biometric tracking to stop fraud before a transaction even processes. This systemic upgrade is designed to heavily target "friendly fraud" and unauthorized chargebacks. For small businesses, this backend shift means fewer disputed funds, lower chargeback fees and a more secure checkout environment without added friction for legitimate buyers.

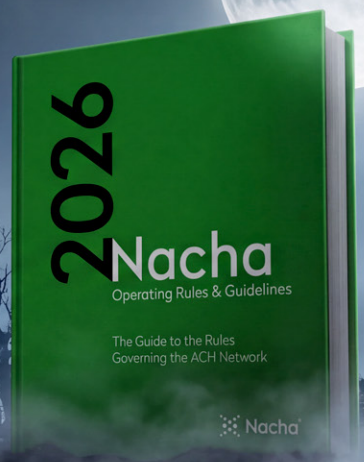
5. High Demand for International Sourcing

A significant macro shift shows that over half of U.S. small businesses now source goods, raw materials or freelance talent from international suppliers. Because global supply chains are no longer exclusive to enterprise corporations, businesses are heavily prioritizing payment networks that offer faster, more affordable international payouts to keep global vendors satisfied and secure preferential pricing.

Don't Let Recent *ACH Rules* Changes Haunt You

The latest *ACH Rules* changes took effect September 18th, including earlier funds availability for non-Same Day ACH credits and an updated definition of an International ACH Transaction (IAT). Don't let these changes become a ghost of your past processes. Revisit our ***2026 ACH Rules Update for Corporate Originators and Third-Party Senders*** for a refresher on these and other 2026 Rule changes.

Download Now!



epcor®
Electronic Payments Core of Knowledge



Fraudsters Have Some Scary Tricks Up Their Sleeves

Fraudsters are constantly conjuring up new ways to deceive, making today's fraud landscape more complex than ever. Our *Did You Know* videos break down some of the latest fraud challenges, including **Fake Banking and Treasury Alert Protection**, **Double-Sided Spoofing**, **First Party Fraud**, **New Fraud Challenges for Third-Party Senders**, **Deepfake Scams** and more!

Check out our other ***Did You Know videos*** for a frightfully good look at today's biggest fraud threats. Uncover the tricks fraudsters are using and share them with your colleagues to help keep your team one step ahead.

epcor®
Electronic Payments Core of Knowledge

THE KILLBUCK SAVINGS BANK CO.
Member FDIC

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.

©2026, EPCOR. All rights reserved.
epcor.org
800.500.0100 | 816.474.5630