

Nacha Toolkit #2

Why Payments Fail: How More
Accurate Data Reduces ACH
Returns, Rework and Risk

Why Payments Fail: How More Accurate Data Reduces ACH Returns, Rework and Risk

In this second installment of our series, we broaden the focus beyond routing numbers to the wider challenge of payment data accuracy. Every ACH transaction depends on a chain of information – from the bank routing number and customer account number and other details – and any weak link in that chain can cause a payment to fail. While many in the industry have long accepted ACH exceptions (failed or returned payments) as an inevitable cost of doing business, the truth is that with more proactive data management, a large share of payment failures are preventable. As modern payments speed up and regulators raise the bar on risk controls, achieving accurate payments the first time has become an operational imperative.

Below, we explore why ACH payments fail and how advanced data validation and verification strategies can drive down exceptions, rework and risk.



Why Payment Data Accuracy Matters More Than Ever

- **Faster Faster payments, smaller error margins:** The rapid adoption of real time and same day payments means there's far less cushion for error. In the past, an ACH payment might have taken a day or two to settle, allowing some time to catch and correct mistakes. But with instant payment schemes like RTP® and FedNowSM, money moves within seconds – and a typo in an account or routing number can result in an immediate failure or worse, an irrevocable misdirected payment. In this high-speed environment, any data flaw must be caught before the payment is released.¹ The pressure is on organizations to perfect their payment data up front.
- **Regulatory crackdown on exceptions:** Rising fraud and error rates in electronic payments have not gone unnoticed. Regulators and industry bodies are increasingly pushing for stronger up-front controls on payment data quality. Since 2021, the Nacha Operating Rules require a consumer account be validated prior to its first use in an ACH debit authorized online (WEB debit), effectively mandating that Originators check new bank account details for validity before any money is moved. This year, Nacha introduced risk-based monitoring Rules obligating financial institutions, third parties, and ACH Originators to monitor for potentially suspicious payments.^{2, 3} Phase 1 of this Rule took effect in March 2026 for high-volume participants, and as of June 2026, every ACH Originator and processor was required to comply.
- **Misdirected payments increase risk:** Not all payment errors result in a straightforward ACH return that can be easily fixed. If an incorrect account number or payee identifier happens to correspond to a real, active account at the receiving bank, a payment might appear to go through – but to the wrong recipient. These misdirected payments can be even more dangerous than standard ACH returns, potentially leading to financial losses and customer disputes. Fraudsters have been known to exploit weak verification processes by tricking employees or vendors into updating beneficiary account details and diverting funds to illegitimate accounts. For instance, recent scam trends include payroll diversion schemes and vendor invoice frauds that rely on changing the payee's bank information to an impostor's account. Without rigorous validation, an organization might unknowingly send money to a fraudster's account, only discovering the error when the legitimate payee complains.⁴ Recovering misdirected funds is often difficult, and the organization may be on the hook for the loss. This is why today's best practices extend beyond preventing outright ACH returns – they also aim to ensure payments are delivered to the correct destination.

Root Causes of ACH Payment Failures

ACH payments can fail for a variety of reasons, but a common thread in most exceptions is bad or outdated data. Understanding these root causes helps highlight where to intervene:

Outdated bank account details:

Customer and vendor bank information doesn't stay static. People and businesses change banks or account numbers, or their banks undergo mergers that alter routing information. If an Originator continues using stale details – for example, sending payroll to an employee's old checking account or to a now-merged bank's retired routing transit number (RTN) – the payment will bounce back. Our first article discussed how maintaining current RTN data is critical to avoiding returns like ACH Return Code R13 (Invalid Routing Number). The same principle applies to account numbers: sending to a closed or incorrect account will trigger a return (e.g., R02 for Account Closed or R03 for No Account/Unable to Locate Account) and delay the payment. A surge in R02 or R03 returns for a particular customer or vendor is often a sign that their banking details on file need an update. Unfortunately, many organizations rely on customers to proactively inform them of changes, or they maintain multiple, siloed databases of bank accounts that easily get out of sync. Without a process to continually refresh these records, it's only a matter of time before transactions start hitting dead ends.

Manual data entry errors:

Whether it's a customer typing their account info into a web form or an employee uploading a payment file, simple typos and transcription mistakes are a perennial cause of payment failures. One transposed digit in a routing or account number can send a payment to the wrong place or to a non-existent account. Despite checksums (like the MOD10 algorithm for RTNs) that catch some errors, many US account numbers lack any built-in check digit, making it hard to detect a bad account number at a glance. In the absence of validation, a form may accept an invalid account number, and the error will only come to light days later when the Receiving Depository Financial Institution (RDFI) returns the entry. In other cases, the mistake passes basic validation but belongs to the wrong person. For example, a hospital that accidentally enters one digit wrong in a patient's refund account could end up crediting a stranger's account – a costly slip-up that might require additional authorization to receive the money back. The risk of human error is amplified when organizations re-key bank data from paper forms or emails, or when customers provide details over the phone. These scenarios lack real-time confirmation of accuracy, meaning errors go undetected until a payment fails or is misdirected.

Inadequate validation or missing information:

Sometimes the problem isn't what data is wrong, but what data is missing. Different ACH payment types have varying data requirements. If a required field is omitted or improperly formatted (for instance, an account number with too many digits, or a missing ID number in certain B2B transactions), the payment may be rejected by the receiving bank or an intermediary. Other failures occur when payments are sent in ways the receiving bank can't accept – for example, using a customer account's routing number to send a Same Day ACH credit, even though the RDFI has only enabled that RTN for wire settlement. These kinds of issues often trace back to misconfiguration or outdated reference data in the Originator's system. They underscore the need for meticulous data governance around payment setup. Every field in an ACH record – not just the obvious ones like routing and account number – should be validated for correctness and appropriateness. Neglecting this can lead to processing rejections or file-level exceptions such as entries that are not processed due to invalid transaction parameters or unsupported payment configurations which then require additional investigation and remediation time.



Upfront Data Validation & Verification: The First Line of Defense

Leading organizations are adopting advanced data validation techniques at the point of data entry and payment initiation to help achieve minimal payment errors. The goal is to verify data before a transaction is sent to the bank.

Key approaches include:

- **Validate bank details at onboarding:** Validating details upfront not only prevents simple errors (such as one-digit typos) from entering the ACH system but also reinforces trust with customers by demonstrating a commitment to payment accuracy. Embedding real-time RTN checks and basic account validation into onboarding and setup workflows has become a widely adopted best practice for reducing exceptions before payments are initiated.
- **Leverage real-time account validation services:** Traditional methods of testing an account, such as sending an ACH prenotification or Micro-Entries, have significant drawbacks – they can take up to three business days to confirm an account, and even then, they don't guarantee the name on the account matches the intended payee. Today, real-time account validation methods are available.

One innovative approach is the “penny test” using instant payment networks: the Originator sends a \$0.01 payment via a real-time rail (like RTP or FedNow) to confirm the account is open and able to receive funds, with immediate acknowledgment of success or failure. Another approach is to query proprietary contributory databases that aggregate account status data from numerous banks. Many Account Status Verification (ASV) services can instantly check if an account is open and in good standing to help reduce the risk of misdirected and fraudulent payments.

For example, LexisNexis® Bankers Almanac® Validate™ Safe Payment Verification (SPV) offers real-time confirmation by verifying personal and business beneficiary account ownership for both domestic and cross-border payments. If an account is found to be closed or invalid, the payment can be stopped before submission, avoiding an ACH return and subsequent remedial work.^{5, 6}

- Verify account ownership and know your payee:** Data accuracy isn't just about numbers and formats – it's also about ensuring the payment is going to the right person or business. Increasingly, banks and corporations are turning to account verification solutions that confirm the payee's identity matches the account on record. Verifying ownership can help prevent certain fraud schemes upfront, for example, a business email compromise that tries to redirect a vendor payment to a criminal's account might be exposed when the payee name doesn't align with the account holder's name on file. Automating real-time account ownership confirmation via cross-checking account details against bank records with a solution such as Bankers Almanac® Validate™ Safe Payment Verification (SPV) helps accelerate Confirmation of Payee requirements in the UK and also streamlines domestic and cross-border payments. While not every ACH transaction today includes payee name matching, this added layer of verification is gaining traction as a powerful tool to reduce "silent errors" where money could otherwise be lost to the wrong party.
- Automate data updates and quality control:** The pace of change in bank account data is only accelerating, which means manual updates and reviews may no longer be sufficient. Wherever possible, automate the maintenance and validation of critical payment data. This includes programmatically updating key reference files (like routing number tables) on a daily or real-time schedule and using software that scans outgoing payment files for errors. Many organizations have implemented payment pre-check routines that automatically compare each outgoing ACH entry against business rules or known issue lists. For example, flagging routing numbers that have recently been retired or account numbers that are no longer present in the official LexisNexis® Bankers Almanac® Routing Transit Number Data solution, which is maintained by LexisNexis® Risk Solutions as the ABA's official registrar, provides more complete and more accurate ABA routing records. Others use intelligent correction tools that can proactively fix common errors such as adjusting outdated routing numbers to their current values based on LexisNexis® Bankers Almanac® Routing Transit Number Data. Taking routine data maintenance out of human hands saves time and helps eliminate the inconsistencies and lags that come with manual processes. The result is a higher baseline of data quality feeding into your payment systems every day.
- Maintain a trusted single source of truth:** One of the most overlooked contributors to ACH payment failures is the fragmentation of bank data across internal systems. In many large financial institutions, different departments or platforms (e.g., treasury, onboarding, fraud and payments) rely on separate sources for routing and transit number (RTN) data, each with its own update cadence and validation logic. This siloed approach leads to inconsistencies in how payments are validated, resulting in unpredictable customer experiences: a routing number accepted in one channel may be rejected in another. To mitigate this, institutions should establish a single, authoritative source of truth for bank data, ideally updated daily from an official registry, and distribute it programmatically to all systems that perform bank data checks. This helps ensure consistency across channels, reduces the risk of false negatives or missed updates and simplifies compliance with Nacha's expectations for data accuracy. Centralization also enables better monitoring and governance, allowing institutions to track data freshness, audit usage and respond quickly to changes in the banking landscape.



Key Takeaway:

Strong data controls help shield the organization from operational, financial and compliance risks that range from customer dissatisfaction and lost opportunities to potential Rule violations and fraud losses. ACH transactions underpin critical business and payroll flows, and their success depends on something as seemingly mundane as correct bank data. The good news is that with modern validation tools and disciplined processes, achieving near 100% first-time payment success is an attainable goal. In an increasingly real time, high-volume payments world, superior data quality translates directly into smoother operations, stronger trust and money that moves to the right place at the right time, every time.

^{1,2} Nacha, Account Validation Resource Center.

³ J.P. Morgan, Preparing for the 2026 Nacha Rule Changes.

⁴ Outseer, 2026 Nacha Rule Change: Proactive Fraud Monitoring Requirement.

⁵ Datos Insights, Account Validation in the U.S. (July 2025).

⁶ LexisNexis Risk Solutions, Safe Payment Verification (SPV).



For more information, call 800 658 5638
or visit risk.lexisnexis.com

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis® Risk Solutions products identified. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc, registered in the U.S. or other countries. Bankers Almanac is a registered trademark and Validate is a trademark of LNRS Data Services Limited. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2026 LexisNexis Risk Solutions.