

Nacha Toolkit #1

How Clean RTN Data Drives
Faster, Safer ACH Payments

How Clean RTN Data Drives Faster, Safer ACH Payments

Routing Transit Numbers (RTNs) are the backbone of the ACH Network. Every ACH transaction relies on an accurate RTN to reach the correct financial institution. Yet despite their critical role, RTNs are often treated as static reference data—set once and forgotten. That approach is no longer sustainable in today's high volume, fast evolving payments environment.

As ACH volumes continue to grow and new payment use cases emerge, maintaining accurate and up to date RTN data is essential to reducing payment exceptions, minimizing delays, and mitigating operational, reputational, and compliance risk.

Why RTN Accuracy Matters More Than Ever

ACH volumes are at record highs with 35.2 billion payments totaling \$93 trillion in 2025, marking increases in both volume and value.¹ This past year marks the 11th consecutive year of trillion-dollar growth for ACH. Same Day ACH credit transfers continue to surge to 1.4 billion transactions in 2025, up 16.7% year-over-year and business-to-business (B2B) payments grew almost 10% to 8.1 billion transactions. With this scale and velocity, even a tiny error rate can impact millions of payments. Each failed payment creates rework and delay; collectively, they impose significant costs and hurt customer experience.



The hidden cost of payment failures:

When an ACH entry is sent to the wrong bank or rejected due to bad data, operations staff must investigate, correct the information and resubmit or reroute the transaction – all of which adds expense. Industry estimates show the cost to remediate a failed payment ranges from \$10 to \$50 per transaction.² These costs add up quickly at scale.

Within the U.S. ACH Network, Nacha enforces return thresholds including 0.5% for unauthorized debits and 3% for administrative errors.³ Exceeding these thresholds may trigger investigations, potential rule violations, fines, and heightened risk scrutiny.

Beyond compliance exposure, repeated payment failures can damage trust if customers are unable to make time sensitive payments such as payroll, bill payments, or loan repayments.

Data Errors Drive Most Payment Exceptions

Payment failures most often originate from incorrect data at the point of entry. Industry analysis consistently identifies outdated or inaccurate routing and account data as a leading root cause of failed ACH transactions, ahead of downstream processing issues.

More broadly, incomplete or incorrect bank data remains a primary constraint on automation across payment networks. Global research shows that average straight through processing rates for cross border account to account payments remain at roughly 26%, meaning nearly three out of four transactions require manual intervention.⁴ Nacha has also emphasized that using outdated routing information will result in failed payments, creating customer dissatisfaction, increasing exception handling costs, and introducing reputational risk for originators and ODFIs.

Poor RTN data hygiene ultimately creates avoidable friction across the entire payments lifecycle. For customers, it can mean delayed paychecks, missed payments, or misdirected funds. For financial institutions, it results in higher costs, increased returns, potential rule violations, and diminished trust.

Common Causes of RTN Data Decay

RTN data degrades over time for several reasons:

Bank mergers, acquisitions, or closures

The U.S. banking industry continues to consolidate. Each year, hundreds of routing numbers are added or retired as institutions merge, receive new charters, or wind down operations. When retired routing numbers remain in use, payment failures are inevitable.

Changes in payment network participation

Financial institutions may join or exit payment networks, change ACH operators, or enable new rails. These shifts can introduce new routing numbers or decommission existing ones.

Branch consolidations and platform changes

Banks regularly consolidate branches or move ACH processing responsibilities, altering which routing numbers apply to specific payment products or regions.

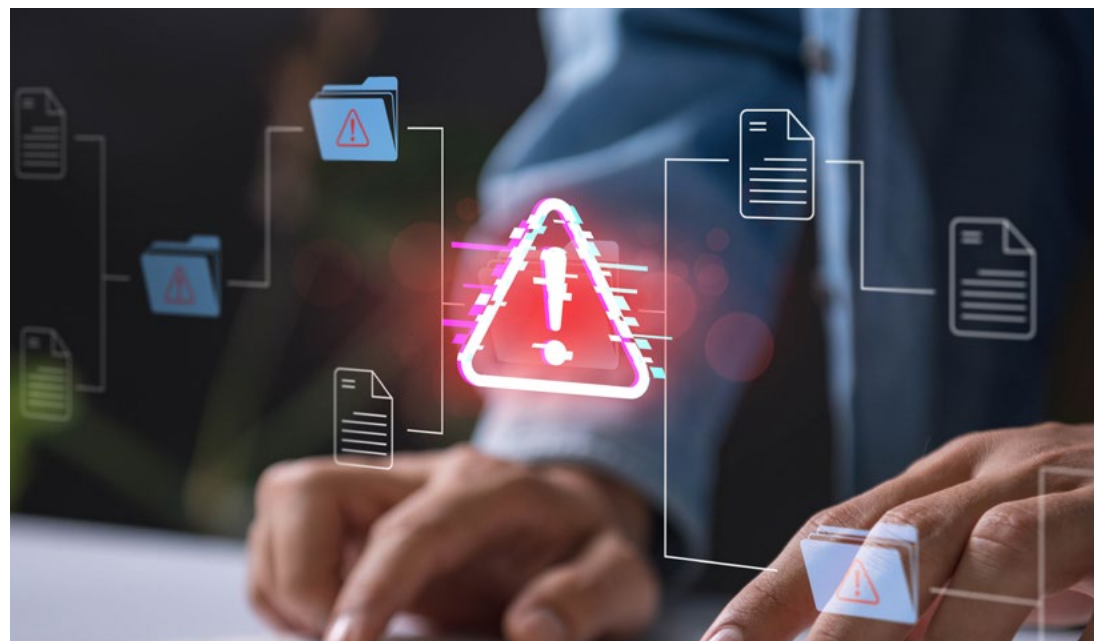
Stale internal reference data

Many organizations rely on static spreadsheets or in house tables to store routing information. Without frequent updates, these repositories quickly become outdated.

Manual data entry errors

Human error remains a factor. Mistyped routing numbers, incorrect drop down selections, or copied data from unreliable sources can easily introduce inaccuracies that evade basic checksum validation.

The good news is that these issues are preventable with the right data practices in place.



Core Best Practices for RTN Data Hygiene

Five foundational best practices can dramatically improve routing data hygiene and, by extension, straight-through processing rates:

1. Use Authoritative Sources – Rely on official, continuously updated RTN data rather than static or self-collected lists

As the official ABA Routing Number Registrar, we maintain the database of all U.S. routing numbers. This ensures that any new routing number assignments, retirements or changes are captured and published in a timely manner. Authoritative data services like LexisNexis® Bankers Almanac® Routing Transit Number (RTN) Data provide current routing information for every U.S. financial institution, with updates available as frequently as daily. Avoid relying on outdated spreadsheets or ad hoc web searches for routing information as those methods are neither reliable nor efficient, especially at scale. Instead, integrate an official RTN data feed or API into your systems, so updates are automatic and consistent.

2. Centralize RTN Management – Maintain a single source of truth for routing numbers within your organization

Fragmented, department-specific reference lists lead to inconsistent updates and confusion. A best practice is to have one enterprise-wide master repository of bank routing details, which all payment applications utilize. Evaluate your environment: if multiple systems store RTN data, consider consolidating them or at least implementing a reconciliation process to keep them in sync. A centralized approach reduces the risk of one system failing to capture an update from other systems.

3. Validate at the Point of Entry – Catch routing errors at the earliest opportunity

When customers or employees input bank routing and account details (for example, during online enrolment for Direct Deposit, or setting up a new biller in an A/R system), the data should be validated immediately. At a minimum, deploy real-time RTN lookup in your user interfaces and internal forms. Ideally, integrate a service that confirms not only that the routing number exists, but that it can accept the payment type in question (ACH credits, debits, wires, etc.). Nacha's Operating Rules mandate certain checks: for instance, any ACH debit authorized over the internet or phone (WEB and TEL entries) must include a "commercially reasonable" method to verify the routing number is valid before initiating the transaction. By validating routing numbers up front, you can prevent typos or outdated information from ever entering your system, thereby avoiding errors before they lead to failed payments.

4. Monitor Routing-Related Return Codes – Use ACH return data as a feedback mechanism for data quality

Pay close attention to returns labeled with codes signaling invalid routing or account issues. For example, ACH Return Code R13 (Invalid Routing Number) or R04 (Invalid Account Number) clearly indicate that the payment failed due to bad bank data. A spike in R13 or R04 returns from a particular batch, customer or business unit should trigger an immediate review of your RTN records and onboarding processes. Many institutions set internal alert thresholds to catch issues early. Typically, these thresholds are set well below Nacha's 3% administrative return rate limit. By tracking return patterns over time, you can identify trends, for example, if a certain new client or software platform is producing an unusual number of R13 errors, you can intervene and correct their data inputs or configuration.

5. Automate Updates and Verification – Don't rely on memory or manual effort to keep data current.

Given that routing number changes may happen multiple times per day, it is best to automate the process of updating and verifying routing information. Utilize direct API calls to pull the latest RTN data from authoritative sources on a frequent basis (daily for high-volume environments, per Nacha's recommendation). Leverage software that automatically checks payment files for invalid or obsolete routing numbers and flags or corrects them before release. Automation not only saves time but also reduces human error.



Embedding Hygiene into Daily Operations

Maintaining RTN data hygiene is not a one-time “cleanup project” – it needs to be an ongoing part of operational excellence. Successful institutions incorporate these practices into their regular workflow:

- Regularly scheduled updates of internal routing tables or databases (with frequency aligned to volume and risk – many large originators update daily).
- Training and awareness for operations and treasury staff about the importance of accurate routing data and how to quickly handle Notifications of Change (NOCs) and other alerts.
- Vendor and software due diligence to ensure any third-party systems (ACH origination software, payment gateways and account validation services) are also keeping their routing data current. If you rely on a software provider, confirm they refresh RTN data at least monthly or better.
- Customer-facing education where appropriate – for example, reminding business customers to alert you when their bank details change, or even providing self-service portals where they can verify and update their own routing and account information.

By making RTN validation and updates part of your regular business strategy, you reduce exceptions without adding friction. As one Nacha bulletin highlights, all parties involved in ACH origination – from ODFIs and processors down to corporate originators – should treat routing number updates as a routine part of payment operations. In doing so, you not only improve your institution’s performance, but you also contribute to a healthier ACH Network with fewer disruptions and less risk for everyone.

Key Takeaways

RTN data accuracy is not just a technical requirement it is a core operational discipline for effective ACH processing. At the scale of today’s ACH Network, even small data lapses can drive significant cost and disruption. By using authoritative data sources, centralizing and automating updates, validating upfront, and monitoring for exceptions, banks and businesses can significantly reduce payment failures. The result is fewer returns, lower operational costs, improved straight through processing, and a better customer experience. Clean routing data lays the foundation for payments that are right the first time.

¹ Nacha, Same Day ACH and Business to Business Payments Propel ACH Network Volume Growth in 2025 (Jan 2026).

² LexisNexis Risk Solutions, True Impact of Failed Payments, 2024.

³ Finextra, Improving Straight Through Processing, June 2021.

⁴ Nacha, ACH Network Risk and Enforcement Topics.



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 of LNRS Data Services Limited, registered in the U.S. or other countries. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2026 LexisNexis Risk Solutions Group.