LexisNexis®
RISK SOLUTIONS

Nacha Toolkit #3

Identifying Red Flags That Indicate Elevated Payments Risk

Identifying Red Flags That Indicate Elevated Payments Risk

The first two articles in this series covered how maintaining clean bank data and validating critical details upfront can drastically reduce avoidable ACH payment failures. In this final installment, we turn to the forward-looking challenge of detecting residual risks and red flags in payment operations before they escalate. Even with strong data hygiene and validation practices, modern payments environments demand continuous vigilance. Real-time monitoring, advanced analytics and cross-functional collaboration have become essential tools for spotting early warning signs of trouble, whether those signs point to potential payment failures, fraud attempts or compliance issues.

ACH payment workflows generate a wealth of data and process signals, which can be analyzed for anomalies. The goal is to surface red flags – indicators of elevated risk that something may be amiss – as early as possible in the life cycle of a transaction. Left unchecked, these subtle warning signs can snowball into hard-dollar costs, from ACH returns to fraud losses or regulatory penalties.

As payment volumes and speed increase, the margin for error shrinks, and the need for automated, real-time detection of problems is critical. Nacha's new 2026 Rules make this official: all ACH Originators, as well as third parties and Originating Depository Financial Institutions, are required to implement risk-based monitoring to detect potentially unauthorized payments, or those authorized under false pretenses.

Why Being Proactive Matters

Rising speed and complexity: The global push for faster payments is relentless. The G20 has set a goal that by 2027 most cross-border payments should clear in under an hour. With initiatives like the RTP® network and FedNow℠, funds can now move in seconds. This is great for customers, but it leaves virtually zero time for after-the-fact corrections. At the same time, the compliance landscape is growing more complex, with an increasing volume of sanctions and evolving standards, such as ISO 20022 for cross-border payments, adding new potential failure points. Many banks and businesses remain constrained by siloed processes and manual controls, making it hard to keep up with this pace. If a payment gets flagged under these conditions, it might already be too late to prevent a failure or fraudulent loss. That's why the industry emphasis is shifting strongly toward proactive exception management. In a recent 2025 survey, over 60% of payment professionals indicated that real-time detection and intervention capabilities are the most critical investments for improving payment integrity going forward.[1]

Regulators are raising the bar: Regulators and industry bodies have taken note of these trends and are embedding proactive risk detection into compliance requirements. Nacha's 2026 fraud risk management Rule is the clearest example: it mandates that all non-consumer parties involved in originating ACH transactions utilize risk-based fraud monitoring.[2] In practice, this means financial institutions and payment processors must implement process and procedures to identify potential red flags, such as suspicious transaction patterns or inconsistencies in payment data. Enforcement of this Rule was phased in over 2026 starting with the largest ACH participants in March and all others by June. Similarly, across the Atlantic, the European Banking Authority has issued guidelines for payment service providers to monitor risk indicators during processing, especially for instant payments, to prevent fraud and errors. These regulatory expectations underscore that early detection of anomalies is now a baseline obligation, not just an internal best practice.

Common Red Flags in Payment Operations

What exactly should organizations be looking for? In broad terms, red flags in payments can be grouped into three categories: operational breakdowns, fraud indicators and compliance issues. Below are some typical warning signs in each category that signal elevated risk or potential failure. Often, these red flags appear well before a major incident – if you know where to find them:

- **Rising exception and return rates:** A gradually increasing rate of ACH returns or payment exceptions over time is a classic red flag of trouble brewing. For example, if your ACH return rate creeps upward toward or beyond Nacha's 3% threshold for administrative returns (R02–R04 series), it may indicate deteriorating data quality or a gap in your customer input process that's letting more errors slip through.[3] A spike in certain return codes (like unauthorized debits, R05–R07 and R10 or R17 (Questionable Transaction) could reveal a weakness in authorization practices or transaction descriptions (e.g., more customers disputing debits they didn't authorize), whereas an uptick in data-related returns (invalid account or routing numbers) points to an internal data management lapse. Monitoring these rates by source, business unit or customer segment can help pinpoint where the problems originate. Leading organizations often set internal alert thresholds far tighter than Nacha's limits, for instance, flagging any week where administrative returns exceed 1% of total volume, so they can intervene long before regulators take notice.

- **Growing manual repair queues:** Another red flag is a swelling backlog of payments requiring manual intervention, sometimes called "payment repair" or exceptions queue. If your operations team is spending more time manually fixing payments – correcting account details, chasing down additional info and resubmitting files – it's a sign that something upstream isn't working correctly. A healthy payment operation sees the vast majority of transactions flow straight through without human touch (STP). Industry benchmarks for cross-border payments, where STP rates have historically been low, show what's possible: in some cases, banks using automated repair and validation tools have achieved 70% to 80% reductions in manual payment repair work.[4] Therefore, if your internal metrics show an increase in manual fixes, duplicate payments being issued to correct errors or a heavy volume of customer inquiries about missing payments, those are red flags signaling the need to double down on upstream data controls or consider new automation for exception handling.

- **Inconsistent routing or approval decisions:** Complexity in payment processing can sometimes mask problems. One subtle operational red flag is inconsistencies in how transactions are handled across different systems or channels. For instance, if the same ACH file yields different results when processed through two separate systems – perhaps one system flags several exceptions that another does not – it may indicate misaligned validation rules or out-of-sync reference data. Likewise, if customer-facing channels (online portals, branch systems, etc.) apply different criteria for accepting or rejecting bank details, you risk unpredictable customer experiences and errors. Consistency is a hallmark of a well-governed payments process. If you observe frequent one-off overrides, ad hoc workarounds or contradictory decision outcomes for similar transactions, treat it as a red flag. It suggests an underlying procedural gap or data inconsistency that should be addressed before it causes a significant failure.

- **Unusual transaction patterns or unusual user behavior:** Red flags are often associated with potential fraud or security issues. Modern fraud schemes, such as business email compromise (BEC) or authorized push payment (APP) scams, may not trigger traditional rule-based alerts if they involve an otherwise legitimate user who has been tricked or compromised. Instead, these require advanced anomaly detection with pattern analysis that goes beyond static payment data. Examples of behavioral red flags include: a sudden rush of first time payments to new recipients, payments made outside normal business hours or from unusual locations/devices or any transaction that deviates markedly from a customer's historical patterns. A classic BEC red flag is when a company that normally pays domestic suppliers suddenly initiates several large international ACH transfers it never made before – often after a sneaky change in instructions by someone posing as a vendor. Modern digital identity and behavioral intelligence tools can build profiles of typical payment behavior for each customer or account and then flag outliers automatically. By detecting these pattern breaks in real time, banks and businesses can intervene in potential fraud scenarios or operational errors that would otherwise slip through.

- **Backlogs in reconciliations or settlement breaks:** Certain back-office issues can indirectly signal elevated payment risk. Regularly unmatched items, delayed reconciliations or end-of-day out-of-balance conditions may indicate payments that were misrouted, unposted or duplicated. These issues often stem from misconfigurations, incomplete data integration or changes to payment systems that are not fully reflected in downstream reconciliation processes. Left unaddressed, such issues can compound over time, increasing operational burden and creating reporting or compliance risk. Early identification through monitoring and internal reviews enables faster remediation of root causes.

Modern Tools for Early Detection

A range of advanced solutions are being deployed to catch red flags automatically and assist humans in making faster, smarter decisions:

- **AI-driven anomaly detection:** The sheer scale and speed of payments today demand automated eyes on transactions. Banks and payment processors are increasingly turning to machine learning (ML) models to detect anomalies in real time. Unlike static rules, ML-based anomaly detection can help detect complex, subtle signals, such as a sequence of slightly unusual events that together suggest something is wrong.[5] For example, an algorithm might learn what a business's typical payroll file looks like in terms of timing, amounts or payee patterns and then flag an instance that deviates significantly, like a file that's much larger than normal or contains a surge of new payees. By constantly adapting to new data, these models can identify emerging threats or process breakdowns faster than traditional monitoring. ML techniques have been used in payments risk for well over a decade. LexisNexis® ThreatMetrix® is powered by tailored models that analyze thousands of fraud signals and autonomously flag suspicious patterns that would elude a human reviewer. As ML capabilities have advanced and become more accessible via cloud-based services, banks of all sizes can implement anomaly detection for their key payment streams without the need for extensive in-house data science teams.

- **Real-time sanctions and fraud monitoring:** Compliance-related red flags, such as sanctions or AML alerts, benefit from early detection. Fast-moving fraud schemes like authorized push payment (APP) fraud and business email compromise (BEC) rely on social engineering to induce legitimate users to initiate payments. These transactions are technically authorized so they can bypass traditional rule-based controls. This underscores the importance of utilizing behavioral signals and upstream verification.

Solutions like LexisNexis® ThreatMetrix®, LexisNexis® BehavioSec® and LexisNexis® Bankers Almanac® Validate™ Safe Payment Verification (SPV) can detect device and behavioral anomalies and help confirm that the payee's name matches the account holder on file, flagging signals that may indicate fraud.[6,7,8] When SPV is integrated into payment workflows, the solution can act as a last-mile defense, especially for high-value or first-time payments, by validating that the destination account truly belongs to the intended recipient. Combined with real-time anomaly detection and sanctions screening, these tools provide a layered approach to fraud prevention and payment accuracy. As instant payments gain traction, regulators and industry bodies increasingly expect 24/7 monitoring and proactive interdiction. The message is clear: if money can move in seconds,
so can fraud — and so must your defenses.

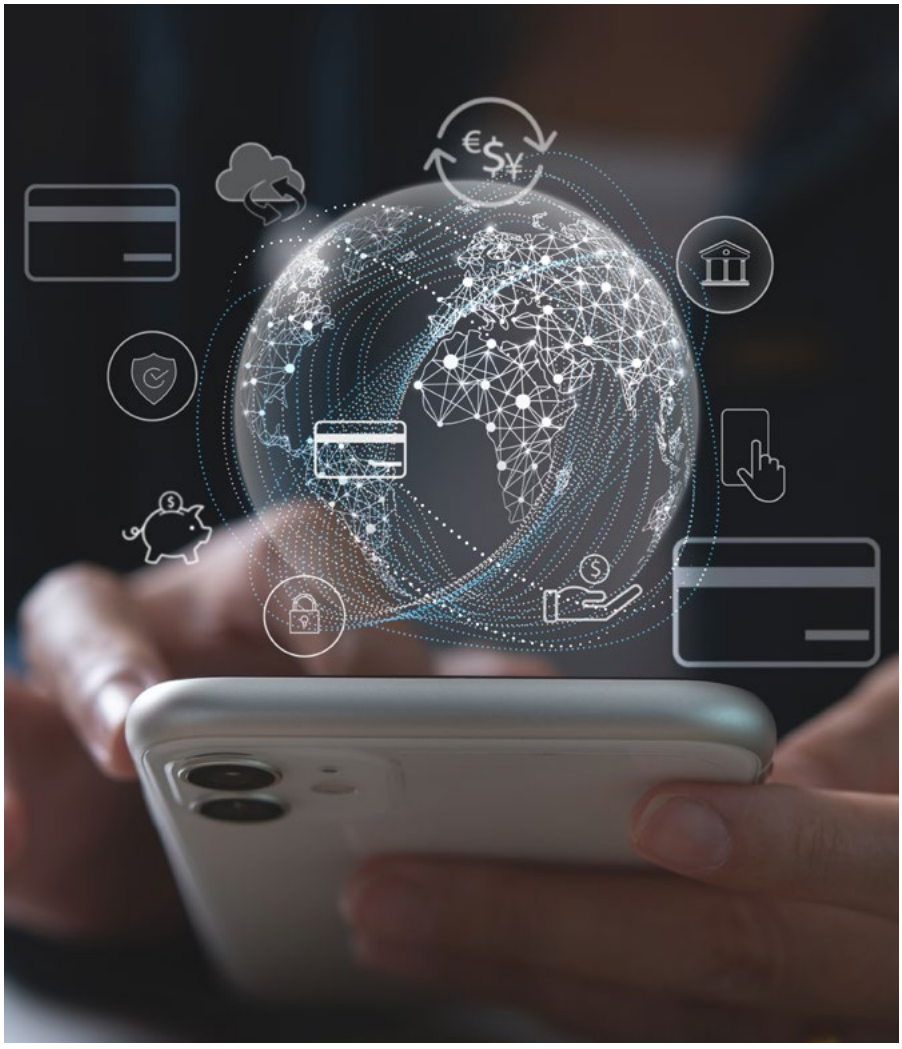
Operationalizing Risk Detection

To fully realize the benefits of early risk detection, organizations should integrate these tools and insights into their day-to-day operations and culture:

- Dashboarding and alerting: An effective way to keep tabs on payment risk is through live dashboards and alerts that surface key metrics and anomalies to the people who can act on them. Modern payment hubs and risk management systems offer configurable dashboards that display current exception volumes, trends in return rates and top causes of failures at a glance. These can be paired with real-time alerts for specific conditions – for example, if the share of ACH payments being held for manual review exceeds a certain percentage in a day, or if a single client's transactions suddenly trigger multiple fraud alerts. By making emerging issues highly visible, dashboards and alerts prompt quicker response. For instance, an ops manager might receive an alert that today's outbound ACH file had an unusually high number of R03 (No Account) returns; upon investigating, they discovered a batch of accounts from a recent client onboarding were all incorrect, leading to an immediate fix of that client's data. The key is to leverage dashboards that are not just for reporting, but for decision support – they should be tied to concrete thresholds and drive action, not simply compile data.

- Exception review drills and feedback loops: Just as incident response teams conduct postmortems, payment teams benefit from regular exception reviews to learn from red flags and refine processes. Some organizations hold monthly cross-functional meetings involving Operations, IT, Risk and Compliance leaders together to review payment errors and near-misses. By analyzing each significant exception or fraud attempt, they identify root causes and ensure that any needed process changes or tech improvements are put in place quickly. Over time, this creates a continuous feedback loop: the more you learn from small red flags, the better you get at preventing the big failures. It's also useful to designate clear ownership of certain alert types – for example, the Fraud Strategy team might own investigating behavioral anomalies and contacting customers if needed, while the Payments Operations team owns remediation of data errors or infrastructure breakdowns. This way, when an alert happens, everyone knows who's responsible for follow-up. A byproduct of such collaboration is a stronger risk culture: employees come to view exceptions not as routine nuisances to be worked around, but as valuable signals of where processes can be improved.

- Empowering people with intelligent tools: Technology is not meant to replace human judgment in payments, but to enhance it. Systems that warn you early work best when they help human operators make faster, more informed decisions. For example, an alert about a possible fraud doesn't help if it just says, "something's wrong" – it should ideally provide context, such as "This payment is 300% larger than this account's average, and the user-device behavioral interactions are suspicious," enabling a risk analyst to act decisively. Dashboards and case management tools should integrate data from multiple sources (ACH returns, fraud scores, customer profiles, etc.) and present a coherent story. With the advances in AI, tools can generate plain-language summaries of complex cases for analysts, or recommend the next best action based on past resolutions to increase efficiency. Training your operations and risk teams to trust and effectively use these intelligent tools is crucial; they need to understand what an alert or score means and how to respond. Providing regular training on new red flag scenarios (e.g., emerging scam tactics) and the capabilities of your detection systems will ensure that your human experts and AI systems together create a robust defense.



Business Value of Early Detection

Investing in robust risk detection and response capabilities yields benefits that go far beyond just avoiding losses:

- Cost savings and efficiency: Perhaps the most tangible benefit of a risk detection strategy is the reduction in the direct and indirect costs associated with payment failures and fraud. Each ACH exception can incur $5–$10 in extra operational expense on average, covering investigation time, customer service and resubmission fees, with complex cases costing significantly more. $5.75 is the average total cost of every $1 of fraud loss for US financial services. Every red flag caught in advance is an exception avoided, meaning that $5 or $50 of cost never has to be spent on fixing a problem after the fact. Moreover, preventing major fraud incidents can yield substantial savings. For every dollar of fraud loss, companies often incur $3 to $4 in recovery costs and associated business losses, from customer churn to legal fees. Early detection is essentially a form of insurance: it's far cheaper to stop a bad payment or correct an error pre-transaction than to deal with the fallout afterward.

- Improved customer experience: Fewer payment problems translate to happier customers and partners. In an age where clients expect seamless, instant payments, being able to catch and resolve issues quickly is a competitive differentiator. Consider two scenarios: In one, a vendor's payment is delayed because of an account number error, and the issue isn't discovered until the vendor complains days later. In another, the error is spotted immediately by an automated check, and the company proactively contacts the vendor to get the correct information the same day, perhaps even sending the payment via a faster rail as a make good. The latter scenario obviously leaves a far better impression. Real examples bear this out. Banks that have implemented real-time payment tracking and exception management have seen their customer satisfaction scores improve alongside reduction in complaints. Proactive alerts, such as "We noticed your payment didn't go through due to an address mismatch; please verify here," not only prevent frustration, they also build trust – demonstrating to customers that their service provider is on top of issues and cares about getting it right.

- Stronger fraud and compliance posture: Finally, early risk detection fortifies an organization's risk management and compliance stance. By catching anomalies early, companies can stop fraud attempts that would otherwise succeed. For example, if an employee's credentials are compromised and the fraud isn't noticed until money is gone, the damage may be irreversible; but if an AI system flags the unusual activity immediately, the account can be frozen before funds are transferred. Likewise, robust monitoring ensures you stay in line with regulations: from meeting Nacha's return rate and fraud monitoring requirements to avoiding OFAC violations. Strong controls can also boost reputational benefits. Regulators and business partners prefer to work with organizations demonstrating a proactive approach to managing payment risk. Conversely, the negative blowback (and potential fines) from a public compliance failure can be devastating. As a commentary on instant payments noted, there is little room for error when money moves in seconds – a major US bank suffering an outage of its real-time fraud filters on a weekend could face penalties of $250 million or more if illicit transactions slip through. The message is clear: the better you are at detecting red flags in real time, the safer your institution and customers will be.

Key Takeaway

Payment operations have come a long way – from reactive error correction to increasingly proactive risk prevention. To achieve the full promise of modern, instant payments, organizations should embrace that next evolution. By harnessing data, analytics and AI to spot risk early, and empowering cross-functional teams to act on those insights, you can prevent many payment failures and fraud incidents before they happen. The result is not only fewer exceptions and losses, but also a leaner operation, happier customers and a stronger compliance record. In the high-speed world of digital payments, success belongs to those who move money quickly and securely – in short, to those who can detect trouble before the money moves.

[1, 4] Pega Systems, Accelerating Resolution of Payment Exceptions.

[2, 3] Nacha, Risk Management Framework and 2026 ACH Rule Updates.

[5, 6] LexisNexis Risk Solutions, ThreatMetrix.

[7] LexisNexis Risk Solutions, BehavioSec.

[8] LexisNexis Risk Solutions, Safe Payment Verification (SPV).

LexisNexis®
RISK SOLUTIONS

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.