

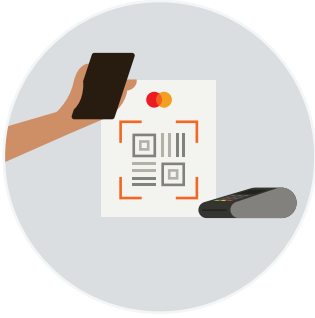


The hidden operational costs of technical debt and legacy systems

WHITEPAPER
AUGUST 2026

Table of Contents

Introduction	3
Where technical debt shows up in card operations	4
Data quality and the true cost of fraud.....	4
Integration friction and the cost of instability	6
Degradation of competitive advantage	8
Opportunity cost of failing to meet cardholders' digital expectations	9
Why this hits community issuers hardest – and why it matters now	10
Three viable paths forward	11
Path 1: Maintaining the status quo	11
Path 2: Incremental modernization via middleware and integration layers	12
Path 3: Full migration.....	13
Conclusion	14



Introduction

Community banks and credit unions depend on relationships and the trust of their customers and members. Many FIs still rely on legacy core and processor infrastructure, a growing paradox that quietly undermines their greatest strengths. A recent industry study found that only half of 100 credit union executives stated that they've reached a mature state of digital transformation to support the digital customer experience (Wipfli, 2025). Processes get repeated year after year, workarounds become normalized and the real cost of operating this way often goes unexamined.

That dynamic shows up as technical debt, which carries real, current consequences. The friction created by technical debt across day-to-day operations quietly degrades the experience for their customers and members, constrains growth and diverts dollars and leadership attention that could be better spent elsewhere. The impact extends well beyond IT, creating an operational drag in the form of resources, controls burden, incident response and slower time-to-market.

This paper focuses on issuer-side card operations, with an emphasis on core banking and card processor technology, viewed through the most important costs that arise and the strategies that can be used to address these issues.



70%

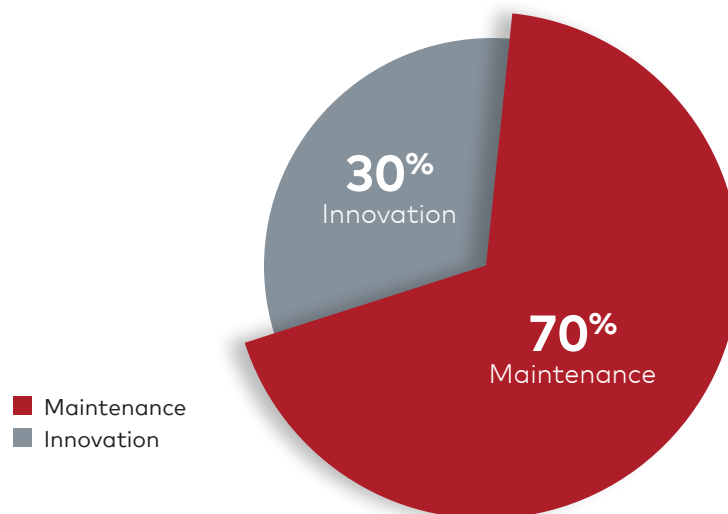
of IT budgets
maintain legacy
systems

Where technical debt shows up in card operations

For FIs, technical debt has become a critical business constraint. Card programs sit at the intersection of fraud risk, cardholder experience, cardholder loyalty and revenue, with the legacy infrastructure that supports them increasing costs at every step. FIs now allocate roughly 70% of their IT budgets to maintaining legacy systems, leaving limited capacity to improve performance or respond to change (RS2 Banking, 2025).

Much of that IT spending functions as ongoing “interest” payments on technical debt: incremental investment as a workaround to outmoded technology rather than fixing the root cause. For community banks and credit unions, smaller budgets and leaner teams amplify the burden as the effect compounds across higher operating expenses, slower execution, and growing risk exposure.

Figure 1: IT Budget Allocation at Financial Institutions



Data quality and the true cost of fraud

Card operations depend on accurate and timely data. When that data is incomplete or delayed, financial impact follows quickly. Fraud signals arrive late, disputes take longer to resolve and staff spend time correcting issues rather than preventing them. To prevent the ensuing backlogs, payments risk guidance recommends minimizing manual intervention and actively managing exception queues. Financial services economics are unforgiving: Every \$1 lost to fraud today translates to \$5.75 in total cost once recovery, compliance and cardholder impact are included, up from \$4 just a few years ago (LexisNexis, 2025). For community banks and credit unions, even a modest volume of fraud can materially erode card profitability.



Many of the costliest gaps are surprisingly basic. Losses attributed to fraud or attrition frequently stem from missing or unusable data. Legacy systems often fail to reliably store or transmit mobile numbers or email addresses, which undermines real-time alerts, digital authentication and self-service controls. The institution pays for those gaps every day through manual intervention and delayed response. While 70% of U.S. financial institutions report mobile fraud has increased by at least 10% in the past year, many legacy environments still cannot support the basic data needed for timely alerts and authentication (LexisNexis, 2025).

Data fragmentation compounds the problem. In Bank Director's 2025 Technology Survey, 56% of banks report keeping data siloed in the systems that generated it, and one-third of bank leaders cite an inability to use data effectively as a top technology challenge (Bank Director, 2025). When cardholder, transaction and risk data live in disconnected systems, even straightforward operational decisions require manual stitching across platforms.

"Legacy systems often fail to reliably store or transmit mobile numbers or email addresses, which undermines real-time alerts, digital authentication and self-service controls. The institution pays for those gaps every day through manual intervention and delayed response."

The same infrastructure gaps that weaken fraud defenses also increase an institution's broader security exposure. When fraud is comprised of transactional losses from bad actors exploiting weak signals, the question becomes whether cybersecurity can defend the underlying platform at all. Legacy systems that cannot support timely patching, modern encryption protocols or end-of-life asset replacement create resilience risk that fraud controls can't offset. The Cybersecurity and Infrastructure Security Agency (CISA) explicitly identifies outdated software as a significant security risk and strongly recommends replacing end-of-life assets and patching critical legacy systems.

58%

of community bankers
rate cyber security
as an extremely
important internal risk

Not all damage appears on a quarterly P&L. In the 2025 Conference of State Bank Supervisors (CSBS) Annual Survey, 58% of community bankers rated cybersecurity as an extremely important internal risk, the highest of any category (CSBS, 2025). That concern is well founded: financial services firms face an average cost of \$6.08 million per data breach, among the highest of any industry (IBM, 2024). Legacy platforms that cannot support timely patching or modern encryption protocols carry exposure that grows with each passing quarter.

44%

of North American financial institutions rely primarily on manual processes while only 20% are mostly automated

Bad data carries a clear price, paid in fraud losses, breach exposure and the operational drag of constant manual correction. Solving for cleaner data only goes so far when the systems that hold it cannot reliably share it. That structural barrier defines the next layer of cost.

Integration friction and the cost of instability

Even when data does exist, it often cannot move cleanly between systems. Community banks and credit unions typically operate inside a web of custom connections built over many years to patch gaps in legacy platforms, with each new enhancement adding a layer of complexity. The impact shows up in staffing models: 44% of North American financial institutions still rely primarily on manual processes, while only 20% are mostly or fully automated (LexisNexis, 2025).

Manual work persists because systems cannot reliably talk to one another. Payments best practices increasingly recommend intraday reconciliation to detect anomalies and recover data faster, yet legacy stacks force end-of-day batch processes, manual matching and spreadsheet controls. In fact, 41% of financial institutions still rely on spreadsheets to manage data used by their own business lines, a workaround that correlates with reporting deadline pressure and data error rates.

Change delivery carries its own hidden tax. Each enhancement triggers multi-vendor coordination and regression testing across interfaces, lengthening delivery cycles and inflating QA costs. Point-to-point integrations built as temporary fixes harden into permanent dependencies, and the underlying economics worsen over time: as the estate fragments, vendor licensing, specialized skill premiums and duplicated tooling all increase. Technical debt also generates recurring interest costs, paid as incremental spend on workarounds rather than as investment in root-cause fixes. Only 33% of banks have fully transitioned to private cloud environments, while 40% continue to operate entirely on-premises (Dedale Intelligence, 2025). The gap between where infrastructure sits today and where it needs to be for effective risk management continues to widen.

The resulting system instability adds a second layer of direct cost. High-impact outages at financial services firms now cost a median of \$2.2 million per hour, 16% above the cross-industry average, with a median detection time of 42 minutes and a resolution time of 58 minutes (New Relic, 2025). For a community bank or credit union running on aging infrastructure with limited redundancy, even a brief disruption to card authorization or online banking can generate losses that dwarf a month's worth of incremental maintenance savings.



High-impact
outages cost
a median of

\$2.2
MILLION
per hour

The burden compounds further in compliance. When systems cannot share data cleanly, staff fill the gaps with manual checks, after-the-fact reviews and signoffs that pile up across the operation. A decade of CSBS survey data shows that the smallest community banks spend 11% to 15.5% of total payroll on compliance tasks, versus 6% to 10% at larger peers (CSBS, 2025). Without clean data lineage across card operations, routine examinations become costly fire drills. The combination of fraud leakage, downtime exposure and compliance overhead means that legacy infrastructure is not simply expensive to maintain; it is actively generating new costs every operating day.

This cost is visible in card dispute handling. When systems cannot share transaction data, cardholder history and case notes in one place, each dispute becomes a manual reconstruction project. Staff pull records from multiple platforms, rekey information into case management tools and chase down details that should already be linked. The result is a hard operational floor: each disputed transaction costs an issuer between \$9.08 and \$10.32 to process, and for every \$13,000 to \$14,000 in annual disputes, one full-time back-office employee is consumed entirely by case handling (Mastercard and Datos, 2025).

When fraud signals arrive on a batch-cycle delay, losses travel deeper into settlement before anyone intervenes. Every missed chargeback window is unrecoverable.

Operational friction is only the start. When core platforms cannot keep pace with market expectations, the cost begins to compound in places that are far harder to recover from.



*When core platforms
cannot keep pace with
market expectations, the
cost begins to compound
in places that are far
harder to recover from.*



Financial institutions that succeeded with modernization report

22%

faster go-to-market speed

Degradation of competitive advantage

The longest-horizon cost of technical debt is revenue that never materializes. Rigid platforms block new card launches, cross-sell programs stall without real-time decisioning and strong employees leave for organizations where they can build rather than maintain. The scale of the missed opportunity is significant and the most consistently underestimated effect.

Rigid platforms block new card launches at exactly the moment community banks and credit unions need to keep pace. Nearly half of Gen Z and millennials intend to move their primary banking relationships, including credit cards, to fintechs (Cornerstone Advisors, 2025). In fact, more than half (59%) of credit union members at the nation's 29 largest credit unions now have checking accounts with other financial institutions (JD Power, 2026).

The institutions winning that share are the ones that are first at launching new card features and product variations. Financial institutions that have succeeded with modernization report 22% faster go-to-market speed and a threefold increase in digital engagement (Capgemini, 2024). Meanwhile, financial institutions on legacy stacks divert a significant share of new product investment to technical debt remediation. The gap widens with every product cycle that passes without a competitive response.

The same delivery constraints hurt cross-sell, which is the highest-margin channel CFIs already have. The marketing ROI of cross-selling to existing cardholders is roughly ten times that of new acquisition (ABA Banking Journal, 2025). Systems that cannot support timely, personalized offers leave that channel largely untapped, and gradually condition cardholders to look elsewhere for the products their primary institution should be offering first.

Technical debt also degrades the institution's ability to attract and retain the people who run the operation. Disconnected systems eat hours in manual data work, and the strongest performers leave for organizations where they can build rather than maintain. In fact, 42% of institutional knowledge is unique to individual employees who hold it (Panopto, 2018), and industry research shows that technical debt accumulates organizational drag in ways that delay modernization until it becomes unavoidable. For CFIs with lean headcounts, that combination quietly compounds every quarter.

The competitive cost is not abstract. It compounds through lost launches, lower engagement and weakened cross-sell, all because of systems that cannot move at the speed the market now demands. Where that disadvantage is most visible, and most painful for community banks and credit unions, is in the cardholder relationship itself.

60%

of consumers would reduce their banking relationship after experiencing fraud

Opportunity cost of failing to meet cardholders' digital expectations

Cardholders measure their experience against what large national financial services providers advertise, and the comparison grows harder to win each year. When core systems cannot reliably pass mobile numbers, even basic capabilities like fraud alerts, instant card controls and push notifications become impossible to deliver. The competitive cost is direct: more than 60% of consumers say they would reduce their relationship with their bank or credit union after experiencing fraud, regardless of who was at fault (Abrigo, 2025). Delayed reissuances, slow dispute resolution and absent push notifications chip away at the relationship advantage smaller financial institutions depend on most.

The infrastructure gap is not abstract. In many cases, building modern customer-facing capabilities for new features on a legacy stack requires customer integration work, multi-vendor coordination across systems that weren't designed to share data and testing cycles that turn routine releases into multi-quarter projects. Even when the budget exists and the business case is clear, the delivery path itself is the constraint. Community banks and credit unions often watch competitors launch features in weeks that take them months to replicate.

Vendor relationships also shape what is achievable on the consumer side. When a processor introduces new capabilities, institutions with API-ready architectures are positioned to adopt them first. Legacy environments require more customization and longer integration timelines, which can delay the cardholder benefits even when the underlying capability is available.

For community banks and credit unions, every unmet expectation detracts from the relationship advantage that is important to maintaining relevancy. Cardholders rarely complain about a slow dispute or a missing alert. They just quietly shift their primary card, move their next deposit or stop opening the app. The damage is invisible until it shows up in attrition, and by then the cost of winning the relationship back is multiples of the cost of keeping it in the first place. Each year of delay widens the gap between what cardholders expect and what systems can deliver.



Why this hits hardest – and why it matters now

Community banks and credit unions face these challenges with fewer resources and less margin for error. The reconciliation, exception handling and integration upkeep that large financial institutions can spread across broad teams falls on much smaller ones. Fragmentation slows fraud response, extends dispute cycles and weakens the cardholder experience.

The timing makes the gap harder to close. Improving operational efficiency now ranks as a top-three strategic priority for credit unions, yet the underlying infrastructure continues to absorb staff time and budget that priority requires (Filene, 2024). Cardholder expectations are not moving at the same speed as FI roadmaps. They are moving at the speed of the largest financial service providers and digital-native challengers, and every year of delay widens the gap between what cardholders expect and what legacy systems can deliver.

The institutions best positioned to act are the ones willing to make a clear, unsentimental assessment of their current infrastructure - where it stops serving the business and what it would take to change that. For community banks and credit unions, the decision is not whether technical debt is a problem worth addressing. The decision is which path forward actually fits their scale, capability and appetite for change.

Improving operational efficiency now ranks as a top-three strategic priority for credit unions, yet the underlying infrastructure continues to absorb staff time and budget that priority requires



47%

of banks are extremely or very satisfied with their core banking system while only

21%

said they were likely to switch providers



Three viable paths forward

Leaders evaluating their technology stack face three realistic options. The right choice starts with a threshold question: where does the constraint actually exist? If the core system is the bottleneck limiting account management, data access or product configuration, then modernization efforts need to address the core. If the processor is restricting transaction routing, authorization logic or network connectivity, then the processor relationship is priority. In many cases, the answer is both, because the two layers are tightly coupled. It comes down to which layer is blocking the capabilities the institution values most and whether the existing vendor relationship can close the gap within an acceptable timeframe.

Path 1:

Maintaining the status quo

Choosing not to act is itself a decision with accelerating consequences. Legacy maintenance costs typically rise 10% to 15% annually as platforms demand more specialized support and more manual effort to satisfy evolving requirements (Digital Bank Expert, 2025). Over three years, a CFI spending \$2M annually on maintenance could see that figure climb past \$2.6M without gaining a single new capability. A major consulting firm found that institutions undervalue the total legacy cost of ownership by 70% to 80% once compliance overhead, integration workarounds and lost opportunity are included (Deloitte, 2024). The status quo is not a holding pattern; it is an accelerating cost curve.

The inertia is understandable but increasingly difficult to justify. An ABA survey found that only 47% of banks are extremely or very satisfied with their core banking system, yet just 21% said they were likely to switch providers (ABA Core Platforms Committee, 2023). That gap between dissatisfaction and action reflects the perceived risk of change, but it also represents a strategic trap. Every year that an institution remains on a platform it's outgrown, the cost of switching rises, the talent pool for maintaining that platform shrinks and the competitive distance from modernized peers grows. Boards that defer the decision are not avoiding risk; they are compounding it.

52%

of executives
say they plan to
modernize with new
services alongside
legacy systems



Path 2:

Incremental modernization via middleware and integration layers

For most institutions, wrapping existing infrastructure in a modern API layer is the most practical starting point. Each new application connects through the middleware rather than requiring changes to the underlying system. The industry has increasingly adopted this approach, focusing on integration before simplification, offering a pragmatic sweet spot to balance the complexity of modernization and implementation.

In a 2024 EY study of financial institutions actively modernizing, 50% had adopted this strategy, and half of all respondents expected to complete their modernization programs within 3 to 5 years (EY, 2025).

Adoption is already widespread. Nearly half of financial institutions surveyed in 2024 reported adding middleware to their stack (CCG Catalyst, 2024), and 52% of executives in a 2025 global survey said they plan to modernize by running new services alongside legacy systems (FIS and TechStudio, 2025).

The initial connection still requires coordination with the core provider, and middleware does not eliminate legacy risk. It contains that risk while restoring near-term agility and preserving optionality for deeper transformation later. This path offers the clearest balance between cost, disruption and measurable improvement in card operations capability.

Sufficient resource capacity and capability in enabling and managing API connections are paramount to ensure success in incremental modernization. A Pacific Northwest credit union that is establishing a novel data lake to support internal efficiencies within its core banking system noted that while APIs improve reliability in modern workflows, they still lack true off-the-shelf readiness and often require extensive customization. Due diligence is key to managing expectations when establishing a clear understanding of transformation efforts during vendor selection.



Modern systems can
reduce IT costs by

30%
to
40%

Path 3:
Full migration

When incremental fixes no longer generate meaningful return and workaround costs exceed the cost of starting over, full migration becomes the right move. Whether the migration targets the core, the processor or both depends, to some extent, on desired outcomes presented in FIGURE 2: FIs should sequence based on which layer creates the most friction against their highest-priority business objectives.

A processor migration may be the right first step if authorization, network connectivity and transaction routing are binding constraints and do not currently exist within existing processor capabilities. When account servicing, data access and product configuration are the bottlenecks, core migration is the priority. In either case, the decision should be grounded in a clear-eyed assessment of where the institution is losing the most value.

This represents a significant investment in dollars and organizational energy. The entire staff participates in testing, training and transition planning over 12 to 24 months, and only about 30% of core transformations over the past decade successfully migrated all ledgers and products to a new platform (McKinsey, 2026). The institutions that succeed all tend to treat migration as an opportunity to redesign workflows and operating models rather than simply replicating old processes on new technology. Modern systems are typically cloud-native. This characteristic can reduce IT operational costs by 30% to 40% through automation and elastic scaling (McKinsey, 2026).

Figure 2: Weighing Incremental Change Across the Processor and Core

	Expected Outcomes	Key Drawbacks
Processor layer	• Faster access to new capabilities without a full switch • Near real-time signals replace batch delays • Live operations stay stable, risk contained	• Capped by the incumbent processor’s roadmap • Integration needs customization and vendor coordination • Legacy risk contained, not resolved
Core layer	• New products and launches without touching the ledger • Siloed core data exposed and usable • Member relationships preserved	Still bound to the legacy core and its terms Quick fixes harden into new debt Access modernized, ledger untouched

TransFund serves as a trusted technology partner that helps bridge the gap between legacy environments and modern payment ecosystems.



To learn more, visit
TransFund.com
and read this article
on *Navigating Being
Network Neutral*



Conclusion

The costs outlined in this paper are constantly changing and are no longer confined to expense lines. They increasingly show up as a point of relevance for financial institutions' retention efforts and long-term competitiveness. Every quarter that action is delayed, maintenance budgets climb, fraud exposure widens and the tools leveraged by digital-first competitors pull further ahead. In fact, digital-native challengers have captured 44% of new checking accounts (Cornerstone Advisors, 2025). Standing still accelerates the distance between a community bank or credit union and where its cardholders expect it to be.

Modernization is not about abandoning what makes community banks and credit unions distinctive. The relationship advantage is real, built over decades of local knowledge and trust that no platform can replicate from scratch. But that advantage erodes when the infrastructure behind it cannot deliver capabilities cardholders now treat as table stakes. Investing strategically in technological modernization enables improving operational efficiency and driving growth, while enhancing the experiences of customers and employees alike.

How TransFund can support: TransFund helps financial institutions modernize their technology without sacrificing the trusted relationships that set community institutions apart. As a network-neutral payments provider, TransFund offers unbiased guidance and flexible access to multiple payment networks, allowing financial institutions to choose solutions based on their unique business goals rather than being locked into a single network relationship. This flexibility enables institutions to optimize costs, improve performance, remain compliant with evolving regulations, and adapt more quickly to changing market demands.

For institutions looking to modernize, TransFund provides a range of future-ready solutions including API integrations, digital issuance, mobile wallets, contactless payments, fraud prevention tools, data analytics, instant card issuance, and cardholder engagement technologies. Because TransFund is core agnostic and can integrate with any core, financial institutions can trust TransFund to reduce reliance on manual processes, enhance security, accelerate product innovation, and deliver the digital experiences cardholders increasingly expect.

Whether an institution chooses incremental modernization or a broader transformation strategy, TransFund serves as a trusted technology partner that helps bridge the gap between legacy environments and modern payment ecosystems. By combining network neutrality, innovative payment technologies, fraud and risk management expertise, and deep knowledge of community financial institutions, TransFund enables banks and credit unions to modernize confidently and remain competitive in an increasingly digital world.



References

Abrigo. (2025). State of Fraud Report 2025.

ABA Banking Journal. (2025, March). Effective Cross-Selling: The Key to Meeting Deposit and Loan Growth Goals.

ABA Core Platforms Committee. (2023, February). Core Platforms Survey.

Bank Director and Jack Henry. (2025, September). 2025 Technology Survey: Banks Grapple With Data, AI Maturity.

BNY and Harris Poll. (2025, October). Voice of Community Banks Survey.

Capgemini. (2024, March). World Retail Banking Report 2024.

CCG Catalyst. (2024, October). New Frontiers in Banking 2024: Balancing Caution and Excitement.

Conference of State Bank Supervisors. (2025, October). 2025 Annual Survey of Community Banks.

Conference of State Bank Supervisors (Siems, T. and Ross, N.). (2025, November). Too Small to Scale: What 10 Years of Data Say About Community Bank Compliance Costs.

Cornerstone Advisors. (2025). Beyond the Paycheck Motel: Strategic Imperatives for Community Banking — 2025 Research Recap.

Cornerstone Advisors. (2025, July). The New Growth Playbook: Vertical and Niche Strategies for Community Financial Institutions.

Cybersecurity and Infrastructure Security Agency. Secure by Design — Guidance on Legacy and End-of-Life Software.

Dedale Intelligence. (2025, October). The Future of Core Banking Survey.

Deloitte. (2024). Banking Survey on Legacy System Total Cost of Ownership.

Digital Bank Expert. (2025, July). True Cost of Delay: TCO, Data Volume, Competitive Edge, and Customization in Legacy Banking System Modernization.

EY. (2025, October). Core Banking Technology Modernization.

Filene. (2024). Improved Operational Efficiencies.



References

FIS and TechStudio. (2025, April). Global State of Bank Modernization & Technology Transformation Survey.

IBM and Ponemon Institute. (2024, July). Cost of a Data Breach Report 2024.

JD Power. (2026, March). U.S. Credit Union Satisfaction Study.

LexisNexis Risk Solutions. (2025). True Cost of Fraud™ Study 2025 — North America.

Mastercard and Datos Insights. (2025, March). 2025 State of Chargebacks Report.

McKinsey & Company. (2022, February). How to Get a Core Banking Transformation Right: Eight Mistakes to Avoid.

McKinsey & Company. Cloud-Native Core Banking Cost Reduction Analysis.

New Relic. (2025, April). State of Observability for Financial Services and Insurance.

Nilson Report. (2025, February). Top 50 Mastercard and Visa Credit Card Issuers in the U.S.

Panopto. (2018). Workplace Knowledge and Productivity Report.

RS2 Banking. (2025, April). How to Solve Banks' Legacy System Challenges While Controlling Risk

Wipfli. (2025, January). State of Credit Unions Report.

