The new payments era

Embracing change at full speed and future-proofing payments for tomorrow's needs

ACI Worldwide®

Table of contents

Introduction: The shifting global payments landscape

In 2030, frictionless, tokenized, intelligent, and truly global payments are a given. Instant cross-border transfers, fraud prevention powered by artificial intelligence (AI), and modular, interoperable payment systems are no longer goals. They're the baseline.

Rewind to the 2020s: The payments ecosystem was at a crossroads. Legacy systems were holding back progress, even as consumer expectations soared and fintech innovation accelerated. Banks, businesses, solution providers, and regulators faced mounting pressure to modernise infrastructure, embrace open ecosystems, and tackle increasingly sophisticated fraud.

This report explores the challenges and strategic shifts—from the rise of AI and orchestration platforms to evolving regulations and modernised payment hub strategies—that are shaping the future of payment systems. It offers actionable insights for all players across the payments ecosystem on how to start positioning themselves today to lead, not lag, as the decade progresses.

Welcome to the origin story of the next era of payments.

Adapt or fall behind: The urgent case for payments modernisation

The PAY360 2025 survey by The Payments Association reveals a sector focused on balancing innovation with operational and regulatory demands. AI stands out as the top opportunity, particularly for fraud prevention and compliance. Cross-border payments remain a key growth area, driven by the push for seamless, regulated global transactions. Regulatory compliance is the leading challenge, while the adoption of new payment methods adds further complexity.

These shifts are happening against a backdrop of rapid transformation. Global payments are changing fast, driven by tech, real-time transactions, digital-first consumers, and fierce fintech competition. Expectations are rising, compliance is tightening, and regulations keep evolving, reshaping the entire landscape. For banks, merchants, and service providers, it's a huge opportunity—but only if they move fast, innovate strategically, and rethink how payments fuel their future.

Traditional systems—rigid and fragmented—can't keep up with the shift to instant, cross-border payments or the need for seamless, secure experiences. Navigating complex global and local rules demands flexible systems, and as digital growth speeds up, so does the need for AI-powered risk management. Legacy tech just can't scale to support new payment methods and partners.

Today, payments aren't just transactions—they're a strategic engine for growth, loyalty, and competitiveness. Businesses need scalable, cost-effective, and flexible tools to streamline payments and ease operational burdens.

Challenges and legacy infrastructure

Banks and financial institutions (FI) face growing pressure to provide seamless, secure, and real-time payment experiences as global demand rises. However, many still rely on legacy systems that are fragmented, costly, inflexible, and hard to scale. These issues block innovation and make integration with modern solutions more difficult. Maintaining outdated systems is costly, limiting investment in new services.

Moving to centralised, cloud-based payment hubs also requires significant investment and brings challenges with security, compliance, and system compatibility. Many existing setups fall short, offering limited coverage, failing to support all payment rails or client segments, and lacking strong analytical tools.

Legacy systems and reliance on multiple vendors also hinder operational efficiency. Banks often deal with manual exception handling and multiple vendor relationships, slowing down operations and increasing complexity. The lack of visibility across systems makes it difficult for banks to make informed, data-driven decisions in real time.

Meanwhile, the payments landscape is more competitive than ever. Non-bank entrants are lowering prices and speeding up time-to-market. Customer expectations are shifting—they want fast, transparent, and unified payment experiences across all channels and geographies. Unfortunately, many banks have customer experience gaps due to inconsistent experiences, slow payment processing, and delayed status updates. Complex authentication processes create friction in what should be seamless transactions. To stay relevant, banks must support the convergence of card and account-to-account (A2A) payments and offer a consolidated view of all payment activity.

Real-time and cross-border payment pressures

The rise of real-time and cross-border payments is reshaping global expectations. Payment volumes are projected to grow from USD 190 trillion in 2023 to USD 290 trillion by 2030, fuelled by global eCommerce and digital transformation. However, slow processing times, high transaction costs, regulatory fragmentation, and fraud risks continue to hold back progress. Meeting demand requires not only speed but also operational resilience and smarter infrastructure. For merchants, this means enabling cross-border payments (including payouts) and adopting unified reconciliation reporting across multiple acquirers. For acquirers and payment service providers (PSP), offering smart transaction routing and intelligent acceptance is becoming essential.

Fraud, risk, and compliance: Getting it right is mandatory

Modernisation is not just about faster payments—it's also about secure payments. Real-time systems have opened the door to sophisticated fraud tactics like Authorised Push Payment (APP) scams and synthetic identity fraud. Losses from APP scams alone are expected to reach USD 7.6 billion by 2028. Traditional fraud defences are no longer sufficient—banks must adopt AI-powered fraud detection, pre-payment screening, and stronger Know Your Customer (KYC) and Anti-Money Laundering (AML) controls. Compliance expectations are also increasing, with Payment Service Directive 3 (PSD3), ISO 20022, and Payment Card Industry (PCI) Data Security Standard (DSS) 4.0 demanding real-time monitoring and adaptive risk controls. Acquirers and PSPs are also focusing on holistic risk management, with pre-built connectors to major vendor solutions that support seamless compliance and fraud prevention across portfolios.

> “A so-called trilemma in payments regulation revolves around combating fraud, enabling instant payments, and protecting privacy—three goals that can be inherently contradictory.
>
> Fighting fraud often requires adding friction to payments, such as suspending or blocking transactions or introducing contemplation periods, which conflicts with the need for instant payments. Alternatively, enhancing fraud prevention may involve more intrusive monitoring, which raises concerns about privacy.
>
> For both legislators and FIs, the key challenge is striking the right balance between these competing priorities.”
>
> **Emanuel van Praag**
> Counsel at Kennedy Van der Laan | Financial Regulatory Law and Professor Fintech and Law

Path forward: Agile, scalable, and interoperable systems

To future-proof their payments infrastructure, banks are shifting from monolithic, single-provider systems to modular, vendor-agnostic solutions. Centralised payment hubs, cloud-native platforms, and industry standards like ISO 20022 are enabling more agile, interoperable operations across multiple payment types. Automation and intelligent tools are becoming essential—not just for fraud mitigation, but also for improving onboarding, exception handling, and customer experience.

Why merchants need to modernise payments

Today's merchants face rising pressure to deliver seamless, secure, and scalable payment experiences across channels and geographies. Consumers now expect frictionless interactions, whether shopping online, in-store, or across borders. But meeting these expectations is becoming increasingly difficult as many merchants remain constrained by legacy systems that are fragmented, inflexible, and slow to adapt.

Merchants struggle with managing multiple provider relationships and integrating payment methods across channels. This complexity—combined with technical challenges, limited payment support, and strict security requirements—leads to inefficient and fragmented payment processes that hinder growth and customer satisfaction.

Additionally, complex reconciliation processes and the need to consolidate data from various systems add to the operational burden.

This complexity is compounded by a surge in fraud risks. As real-time and cross-border payments become more widespread, fraud threats have grown more sophisticated, often fuelled by AI and generative AI (GenAI) technologies. According to the latest Global Payments and Fraud Report by Merchant Risk Council (MRC), a significant share of merchants are grappling with top threats such as real-time payment fraud, refund and policy abuse, phishing, card testing, and first-party misuse. These threats are no longer just security concerns—they have direct implications on customer experience and operating costs.

Reducing fraud and chargebacks remains the top priority for fraud professionals, but there's a noticeable shift in focus: operational efficiency has become just as important. Many merchants now recognise that the cost of fraud management itself must be addressed. Manual processes are declining, and there's been a steady move toward automation and digital screening. In fact, merchants are screening fewer orders manually than in previous years, and when they do, about 20% are declined—a rate that holds steady across regions and merchant segments.

The rise of AI—especially GenAI—is reshaping fraud management. More than half of merchants already use these tools, with more planning adoption soon. Yet, challenges remain: more than 80% report issues with data and technology, from using data effectively to improving AI/machine learning (ML) accuracy and coverage. As fraud evolves, merchants are struggling to keep up, underscoring the need for adaptable, forward-looking strategies.

Looking ahead, 63% of merchants plan to increase fraud tech investments, while only half will grow staffing. The focus is shifting to scalable, AI-driven solutions to reduce fraud losses, streamline operations, and protect customer experience.

There's urgent need for infrastructure that is both secure and agile. For enterprise-level merchants with global operations, optimising acceptance across currencies, regions, and local payment methods is now foundational to success. Many are turning to payment orchestration platforms that intelligently route transactions, reduce costs, and maximise approval rates. Meanwhile, technologies like tokenization are becoming central to enabling recurring payments, enhancing security, and streamlining omnichannel checkout.

In the end, modernising payments is about more than keeping pace with customer demands or fighting fraud. It's about building a foundation that drives efficiency, trust, and long-term growth in an increasingly complex global environment.

Adapting to the future: What billers must prepare for

Billers face growing challenges as digital and real-time payments become the norm. Many still rely on outdated systems, with high paper check volumes and limited payment options. Operational inefficiencies—such as manual reconciliation, complex integrations with legacy platforms, and poor digital adoption—strain resources. Additionally, compliance requirements, including sanctions screening, add pressure.

A shift toward modernised payment systems is helping billers consolidate infrastructure, improve payment visibility, and gain better insights into customer payment histories. Advanced exception handling, such as real-time payment posting and automated return management, is streamlining processes, reducing friction, and lowering return handling costs. This transition helps billers improve payment collection and customer management while addressing operational challenges and enhancing digital capabilities.

Looking ahead: Framing the future of payments

The next five years will bring a wave of transformation to the payments ecosystem, driven by rapid advances in technology, evolving regulations, and shifting consumer expectations. This paper explores the trends that are poised to redefine how money moves, how trust is built, and how value is exchanged in an increasingly digital economy.

This report asks a central question:

What will the payments ecosystem look like in 2030—and how can organisations position themselves today to lead, not lag, in that future?

To explore this, we break the question into two core areas:

- **Imagining payments 2030:** What will the future of payments look like? What new technologies, regulations, and consumer behaviours will shape the landscape? And how might the architecture of financial services evolve?
- **Strategic readiness:** What steps can banks, merchants, billers, and solution providers take now to build resilience and agility? How can they turn uncertainty into opportunity, leveraging emerging tools while staying compliant and competitive?

By blending expert insights from key leaders in the payments space with forward-looking analysis, this paper offers a practical roadmap for navigating what's next. It empowers all players in the payments ecosystem to rethink strategy, embrace innovation, and stay ahead in a fast-moving industry.

Rebuilding banking from the core: The strategic case for payment hubs

Why payments are the battleground

Payments are no longer just a back-office function. They have become a primary touchpoint in the customer experience and a significant driver of strategic differentiation for banks. In a world of real-time expectations, embedded financial services, and intelligent automation, the ability to process payments swiftly, securely, and intelligently is now a core requirement.

Yet most banks remain encumbered by legacy infrastructure: siloed systems for different payment types, rigid processing logic tied to proprietary clearing schemes, and overlapping layers of compliance and risk management tooling. These operational silos have become a drag on innovation, efficiency, and scalability. Meanwhile, digital-native competitors are using flexible, cloud-native platforms to launch new products, integrate seamlessly into third-party ecosystems, and respond to shifting market dynamics at speed.

According to McKinsey, banks that modernise their payments infrastructure can achieve a 15–20% increase in revenue and a 25–30% reduction in operational costs. This dual value proposition—revenue growth and cost containment—makes payments modernisation a board-level strategic priority.

> “Payment hubs are critical for banks to modernise and stay competitive in a rapidly evolving financial landscape. Streamlining cards, A2A, cross-border, digital assets, etc., improves efficiency, scalability, and customer experience, while continuing to meet rising regulatory challenges in a highly competitive, tech-driven landscape. Payment hubs also offer a new inroad into the world of Open Finance, servicing payment functionalities in the growing number of payment situations in our digitising world. The zero option—not using payment hubs—risks ceding ground to agile fintech players and innovative SaaS providers that integrate payment functionality and, in doing so, become the primary payment interface. Inaction invites disruption.”
>
> **Douwe Lycklama**
> Senior Vice President
> INNOPAY—a business of Oliver Wyman

From fragmentation to flexibility

Most banks still operate fragmented systems tied to individual payment rails (card networks, Swift, ACH, SEPA, RTGS, and more), each with unique formats, compliance rules, and fraud protocols. The result is a redundant infrastructure, slow innovation cycles, and inconsistent experiences. These silos are increasingly unfit for real-time, integrated service delivery.

The strategic role of payment hubs

A payments hub is more than just a piece of middleware or a tool for routing transactions. It is a foundational architecture that enables banks to decouple payments processing from individual schemes and channels, allowing for consistent business logic, centralised monitoring, and unified customer experiences.

Datos Insights defines a payments hub as a centralised platform that processes and manages all payment types across the institution. It acts as a single point of integration for upstream systems and a unified interface to downstream clearing networks. But beyond architecture, the payments hub represents a strategic shift toward platform thinking in banking, one that supports agility, modularity, and scale.

According to Datos Insights’ 2023 report, 97% of payment executives expect their payment business to grow in the next two years, with 44% anticipating significant revenue increases. Capturing that growth requires a fundamental transformation in how banks process and deliver payments. Payment hubs are increasingly seen as the enabler of that transformation.

What payment hubs enable: Strategic capabilities

Centralised payment hubs unlock a range of capabilities that align directly with the goals of modern banking leadership. From a growth perspective, unified platforms enable banks to launch new products faster across all payment types, while also improving the customer value proposition with integrated APIs and consolidated cash management offerings. The ability to quickly onboard fintechs, corporates, and new clearing partners opens up new market segments and revenue streams.

Payment hubs also eliminate redundant systems and standardise processing, which lowers costs and reduces operational friction. They enable higher levels of automation, limiting manual intervention and improving accuracy. Centralised visibility across payment types helps banks identify and resolve bottlenecks in real time, improving performance and service.

Cost benefits are further enhanced when payment hubs are deployed on modern, cloud-native infrastructure. Cloud platforms minimise the need for large on-premises investments and allow banks to scale capacity up or down as needed. Centralising compliance, monitoring, and reporting functions reduces duplication and lowers the total cost of ownership across the enterprise.

From a compliance standpoint, payment hubs simplify the application of controls like fraud detection and AML checks. Policies can be configured once and applied enterprise-wide. Native ISO 20022 support ensures global standards alignment, while end-to-end traceability simplifies audits.

Customer experience is perhaps the most visible area of improvement. A central hub enables a unified view of customer payment activity, speeding issue resolution and enabling more personalised services. For corporates, managing all payments through a single interface improve control and transparency.

The breaking down of historical divides

Traditionally, card payments and account-based payments have been treated as separate domains, with distinct platforms, governance models, and product teams. But this separation is increasingly outdated.

The rise of open banking, digital wallets, and embedded finance is creating convergence across these payment types. Consumers and businesses expect consistent experiences regardless of rail or channel. Payment hubs that support multi-rail orchestration; handling cards, A2A, crypto, and other instruments on a single platform, are becoming critical to delivering those experiences.

Datos Insights finds that a growing number of banks implementing payment hubs are explicitly including card payments in their scope. This convergence is not only technically feasible but increasingly seen as commercially necessary.

AI and cloud: Accelerators of change

The power of a payments hub is multiplied when combined with cloud-native infrastructure and AI. Cloud enables dynamic scaling, rapid deployment, and seamless integration with third-party services. AI enhances fraud detection, supports intelligent routing decisions, and enables proactive risk and liquidity management.

Experts highlight that businesses using AI in their payment operations are seeing up to 40% improvement in fraud detection rates and 25% reductions in false positives. When applied across a centralised hub, these capabilities can be embedded consistently across all transaction types and customer segments.

Moreover, cloud-native hubs enable banks to respond in real time to changes in payment volumes, clearing partner status, or regulatory rules, providing the kind of operational agility that legacy systems cannot match.

Architecting for the future of payments

The long-term strategic value of a payments hub lies in its ability to evolve. As new schemes emerge, digital currencies mature, and open finance accelerates, a hub-based architecture that allows banks to plug in new capabilities without overhauling their entire payments stack.

Future-ready hubs support multi-rail orchestration, including real-time, high-value, cross-border, and card networks. Smart routing capabilities allow payments to be directed based on cost, speed, risk exposure, or customer preference. AI-driven decisioning enhances fraud detection, liquidity management, and exception handling. Integration with broader ecosystems, via secure APIs, enables banks to deliver Banking-as-a-Service models and partner-driven growth. And because payment hubs are built for modularity, banks can compose new offerings from existing services rather than starting from scratch each time.

Strategic considerations for executive teams

For executive teams, payment hubs represent a strategic capability, not just an IT upgrade. The opportunity is not only to simplify operations, but to reshape the bank's competitive position in a digital-first market.

Modernisation efforts should align with broader business objectives, not be treated as compliance exercises. Priorities include breaking down silos between payment types, delivering unified customer experiences, and using AI and cloud as essential enablers.

Finally, executive teams must ensure the architecture is designed for extensibility. Payment innovation will not slow down. Hubs must be able to evolve as new standards, schemes, and business models emerge. A payments hub is not a static platform—it is a foundation for continuous reinvention.

The future of cross-border payments: Real-time transactions driving global growth

Global payment volumes are rising fast, driven by digital adoption, eCommerce growth, real-time payments, and digitised commercial flows. At the same time, competition is heating up, pricing is under pressure, and FIs face higher costs as they try to scale, fight fraud, and keep up with compliance.

Therefore, transforming how payments are supported is a high priority for FIs, with many ranking it among their top three enterprise initiatives and allocating significant funding. Datos Insights' research shows that 94% of bank payments executives expect their institutions to make moderate to significant investments in payments technology over the next 24 to 36 months for commercial and retail payments.

The global cross-border payments market is projected to grow significantly, from USD 190.1 trillion in 2023 to USD 290.2 trillion by 2030. Key drivers include wholesale payments—expected to increase from USD 149.1 trillion to USD 230.8 trillion—and B2B transactions, forecasted to rise from USD 39.3 trillion to USD 56.1 trillion. Consumer cross-border payments are also set to nearly double from USD 1.7 trillion to USD 3.3 trillion, driven by eCommerce, digital wallets, and remittances.

Several key trends are accelerating this growth. The demand for real-time payments and interoperability is rising as businesses and consumers seek faster, more seamless transactions. At the same time, the adoption of digital payment solutions—powered by AI, smart routing, open banking, and cloud-based infrastructure—is transforming the landscape. These innovations are making cross-border payments more cost-effective and efficient by enabling faster settlement, reducing fees, improving FX management, and streamlining compliance.

Other key trends driving the growth of cross-border payments include:

- The rise in international trade, with global trade value reaching USD 24.9 trillion in 2022
- The growth of remittances, which increased from USD 100 billion to USD 550 billion between 2000 and 2019
- The expansion of cross-border eCommerce, projected to reach USD 7.9 trillion by 2030
- The growth of the sharing economy, expected to grow from USD 387.1 billion in 2022 to USD 827.1 billion by 2032

Faster, cheaper, and more inclusive cross-border payments

Despite this growth, traditional cross-border payment systems have long been plagued by inefficiencies. Transactions are often slow and expensive, requiring multiple intermediaries and taking several days to settle. These challenges stem from high costs, slow processing times, and a lack of transparency due to fragmented infrastructure. As a result, complexity, fraud risks, and currency fluctuations remain significant concerns.

Advancements in financial infrastructure and regulatory support, along with technologies such as blockchain and Swift's gpi, are transforming the industry. These innovations are enhancing speed, reducing costs, and improving transparency, making cross-border payments more reliable and efficient.

In this context, in 2020, the G20 launched an ambitious roadmap to overhaul cross-border payments by 2027, addressing high costs, slow speeds, limited access, and lack of transparency. Led by the Financial Stability Board (FSB) and supported by the Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures, the initiative sets clear, measurable targets across four key pillars: cost, speed, transparency, and access. It aims to make cross-border payments cheaper, faster, more inclusive, and more transparent, while also supporting remittances, strengthening economic resilience, reducing reliance on outdated systems, and expanding participation in the global digital economy.

> “As client expectations evolve, we have seen a surge in cross-border payment initiatives in recent years. While this progress is encouraging, the sheer breadth of development—and the potential for duplication—risks adding further complexity and fragmentation. To counter this, the ***G20 Roadmap for Enhancing Cross-border Payments***, with its clear targets to lower costs and increase the speed, accessibility, and transparency of international payments by the end of 2027, plays a key role. It serves as a guiding framework to help ensure the industry moves in the right direction.
>
> However, without regulatory mandates, its success depends on collective, consistent, and well-resourced industry action. Achieving this requires a mindset shift: We should not view it merely as a compliance effort, but as a real opportunity for the industry—both from a private and public sector perspective—to shape its own destiny and, ultimately, meet the needs of end customers.”
>
> **Marc Recker**
> Head of Client Solutions and Partnerships
> Institutional Cash Management
> Deutsche Bank

4 key pillars

Cost **Speed** **Transparency** **Access**

Key G20 targets:

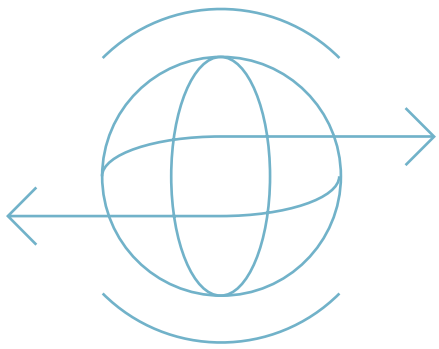
Cost:

- **Retail payments:** The global average cost of a cross-border payment should be no more than 1%, with no payment corridor exceeding 3% by the end of 2027.
- **Remittances:** The global average cost of sending USD 200 should be no more than 3% by 2030, with no corridor above 5%.

Speed: At least 75% of cross-border payments—including wholesale, retail, and remittances—should deliver funds to recipients within one hour of initiation. The remainder should be settled within one business day.

Transparency: All service providers must disclose total transaction costs, expected delivery times, and payment tracking capabilities.

Access: By 2027, all end-users—individuals and businesses—should have access to at least one infrastructure or provider for sending and receiving cross-border payments.



Global real-time payments: A rapidly evolving landscape

Real-time payments are no longer an emerging trend—they're a global force. In 2023, real-time transactions surged to a record 266.2 billion, marking a 42.2% year-over-year growth. Real-time payments systems are now available in more than 100 countries, with 575 billion real-time payments expected by 2028, representing 27% of all electronic payments globally. The demand for real-time payments is growing beyond domestic transactions, with cross-border payment systems gaining momentum.

> The future of real-time payments is exciting but also complex. We anticipate the continued expansion of over 100 instant payment systems globally, while interconnectivity models will continue to flourish and compete, providing significant progress for Global Transaction Banking and augmenting the need for alternative technologies and asset types. Further, instant payments will continue to challenge the rest of our financial market infrastructure, pushing the need for continuous settlement, availability of foreign exchange, liquidity of various assets, and working capital tools to match. At BNY, we're excited to be leading this charge and setting a new foundation of services for the market to innovate upon."
>
> **Carl Slabicki**
> Executive Platform Owner, Treasury Services at BNY

Fuelling factors

- Mobile wallet adoption is strongly linked to real-time payment growth—91% of Indian, 90% of Indonesian, and 87% of Malaysian consumers used mobile wallets in 2023.
- Cross-border ambitions are gaining traction, especially in Asia, with regional collaborations improving interoperability and access.
- A constant flow of user-friendly use cases, open ecosystems, and merchant incentives—such as India's QR code push and zero MDR policy—are also key to adoption.

Real-time cross-border payments are becoming a crucial expectation for businesses. In today's fast-paced environment, companies demand the same immediacy in international transactions as they do in domestic ones. As global commerce continues to evolve, seamless and real-time cross-border payments will become essential for businesses and consumers alike.

> Cross-border real-time payments are approaching a major turning point. While domestic real-time systems have become standard in many markets, achieving instant, seamless cross-border transactions will require industry-wide collaboration across banks, fintechs, and regulators to align on standards, compliance frameworks, and data requirements. Clients are increasingly viewing real-time cross-border payments as the norm, not the exception. When (not if) our industry delivers on this vision, it will further accelerate the growth of global commerce."
>
> **Manish Kohli**
> Head of Global Payments Solutions
> HSBC

Businesses and consumers increasingly prioritise speed, efficiency, and transparency, driving the adoption of real-time solutions. Expanding cross-border real-time payments is a major opportunity to strengthen global financial connectivity by building on existing domestic payment systems.

Interlinking domestic real-time payment systems with international ones is central to the G20's vision of faster, 24/7 cross-border payments, amid rising pressure to improve real-time payment capabilities across borders.

Global initiatives like Swift's gpi—along with regional efforts such as Europe's SEPA Instant, Brazil's Pix, India's Unified Payments Interface (UPI), and the U.S.'s FedNow® and RTP systems—are laying the foundation for real-time cross-border transactions. Fintech innovations are further accelerating this shift, making international transfers faster, more seamless, and more accessible.

As countries work to interlink their domestic schemes, cross-border payments are becoming increasingly seamless. The growing interoperability between real-time payments, central bank digital currencies, and digital assets will further simplify transactions between traditional bank accounts and digital currency accounts.

Markets leading in real-time payments adoption

India leads the world in real-time payments, with 129.3 billion transactions in 2023, accounting for 84% of the country's electronic transactions. Brazil has experienced rapid growth, driven by Pix, with 37.4 billion real-time transactions. Thailand follows with 20.4 billion transactions, while China and South Korea recorded 17.2 billion and 9.1 billion transactions, respectively.

Rapid-growth markets like Egypt, Peru, Croatia, Portugal, Ireland, and Pakistan are early in their real-time payment journeys but are seeing explosive growth, with CAGRs ranging from 52.1% to 110.3% through 2028.

Regional market highlights

The Asia-Pacific region leads the global real-time payments market, with 185.8 billion transactions in 2023. It's also at the forefront of cross-border real-time payments, highlighted by initiatives like the Asian Payment Network and Project Nexus.

The Middle East is the fastest-growing market, projected to see significant growth by 2028, with a CAGR of 28.8%. Europe's real-time payments volume is expected to rise following the EU Instant Payments Regulation (IPR). North America is seeing major growth, fuelled by The Clearing House's RTP system and the U.S. Federal Reserve's FedNow service. Africa leads with the highest share of real-time payments, at 40%, with Nigeria at the forefront. Latin America continues to modernise real-time payments, pushing forward with key initiatives such as Colombia's Bre-B.

Worldwide, common use cases are emerging as countries progress, including merchant payments via QR codes, government disbursements, and Request-to-Pay solutions for bill payments, including future transaction scheduling.

Real-time payments: A catalyst for financial inclusion and economic growth

According to ACI Worldwide's Real-Time Payments: Economic Impact and Financial Inclusion report, the global impact of real-time payment systems is already substantial. In 2023 alone, real-time payments supported USD 164 billion in GDP across 40 countries, equivalent to the labour output of 12 million workers. By 2028, this impact is expected to grow to USD 285.8 billion, a 74.2% increase, representing 16.9 million workers' output.

In the five leading real-time payment markets—India, Brazil, China, Thailand, and Mexico—real-time payments delivered USD 99.6 billion in business and consumer benefits in 2023, supporting USD 114.6 billion in GDP (0.43% of combined GDP). These numbers are forecast to rise to USD 199.7 billion in benefits and USD 188.1 billion in GDP by 2028, representing 0.56% of combined GDP, or the economic output of 13.2 million workers.

Even in developed economies—such as the U.S., Canada, the U.K., France, and Germany—the impact is growing. In 2023, real-time payments supported USD 2.9 billion in benefits and USD 9.7 billion in GDP (0.03% of combined GDP). By 2028, these figures are projected to climb to USD 8.1 billion in benefits and USD 17.7 billion in GDP, equivalent to the output of nearly 145,000 workers.

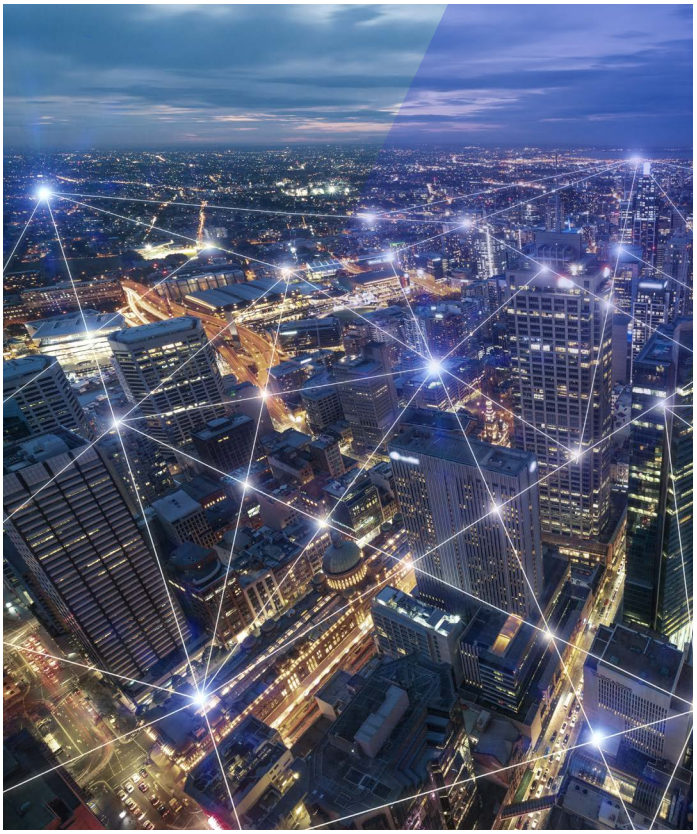
Beyond enhancing business efficiency, real-time payments are playing a pivotal role in advancing financial inclusion. By enabling fast, accessible, and secure transactions, they open financial opportunities for underserved populations—such as gig workers, small merchants, and street vendors—who often lack access to traditional banking services.

This trend is especially evident in developing economies across Asia, Latin America, and Africa, where there's typically lower reliance on credit and debit cards. In these regions, real-time payments are emerging as a powerful tool for digital financial inclusion. By offering an easy-to-access payment solution, they allow more individuals and businesses to participate in the formal economy, ultimately fuelling broader economic growth and stability.

The financial inclusion benefits are particularly pronounced for young adults, women, and low-income groups. By 2028, it's estimated that 167.2 million previously unbanked individuals across 28 countries could gain access to formal banking services through real-time payment networks. Looking closer at inclusion metrics, between 2021 and 2028, countries such as Pakistan, the Philippines, India, China, and Nigeria are expected to see 138 million newly banked individuals-roughly 4.1% of their combined populations.

Beyond economic growth, real-time payments improve transparency, reducing fraud and money laundering, and accelerate the shift toward a cashless economy. To stay competitive, FIs and PSPs are expanding their real-time payment capabilities to meet rising demand from businesses and consumers.

With these clear advantages, it's no surprise that governments worldwide are prioritising real-time payments as a powerful tool to increase economic growth and financial access.



Real-time payments and the merchant opportunity

The opportunity for merchants is transformative. Real-time payments enable instant settlement, reducing cash flow delays and improving working capital management. They also reduce reliance on costly card networks and eliminate waiting periods tied to traditional banking rails.

In markets like India and Brazil, government and central bank incentives have driven explosive real-time payment adoption among merchants. India's UPI success, powered by QR codes and a zero MDR policy, showcases the potential when infrastructure and incentives align. Similarly, Brazil's Pix system has seen widespread merchant uptake thanks to its seamless integration with mobile and online commerce.

Juniper Research projects that consumer instant payments will grow 218%, from 74 billion in 2023 to more than 235 billion by 2027, as merchants look for lower-cost alternatives to card networks amid economic pressures. Instant payments—those processed outside card networks in under 10 seconds—are expected to account for 70% of all consumer payments globally by 2027, up from just over 30% in 2023. The fastest-growing markets are China (led by WeChat Pay and AliPay), India (via UPI), and the U.S. (driven by the launch of FedNow).

In Europe, initiatives like Wero—a digital wallet solution launched by European banks to facilitate pan-European payments—are emerging as strategic responses to merchant needs. Wero is positioned to serve both consumers and businesses by offering real-time, low-cost transactions across borders, and as it scales, it could significantly boost real-time payment adoption across retail and commercial sectors in the EU.

As Martina Weimert, CEO of EPI Company, explained that Wero, EPI's mobile-first wallet, is specifically designed to meet merchants' growing need for a robust alternative to card-based payments—one that can handle the complexity and diversity of today's European market. Merchants, especially those operating internationally, currently face a fragmented landscape with varying national payment systems, rules, and business models, which complicates cross-border transactions and increases operational burdens.

Wero addresses these challenges by offering a unified, pan-European digital wallet that enables seamless instant payments across borders, backed by major European banks for widespread adoption. With a roadmap that includes an eCommerce market launch in summer 2025 and future features like Buy Now, Pay Later and loyalty programs, Wero promises to simplify merchant operations, reduce costs, and foster broader adoption of instant payments, ultimately streamlining commerce and enhancing competitiveness across Europe.

> “Instant payments—the ability to transfer money within seconds—is set to reshape treasury processes. Following the introduction of the first stage of the EU IPR in January 2025, we are already seeing a rise in instant payment volumes. This growth is driven not only by consumers but also by companies increasingly adopting this payment method—particularly those in business-to-consumer sectors.
>
> However, we expect real-time payments to become even more relevant for B2B business models and treasury payments. In October 2025, when the EUR 100,000 upper limit for SEPA instant payments is removed, treasurers will gain the ability to use instant payments for supplier, M&A, license, and tax payments, which often exceed the current threshold.
>
> A major advantage of instant payments is that they eliminate the early cut-off times of traditional ACH and high-value payment systems. By enabling treasury teams to execute transactions later in the day, instant payments enhance liquidity management, reduce reliance on short-term credit, and simplify cash forecasting.”
>
> **Christof Hofmann**
> Global Head of Corporate Cash Management at Deutsche Bank

The EU IPR, alongside Wero, is set to transform the European payments landscape. As of 9 January 2025, all EU banks must be able to receive instant payments, pushing major infrastructure and operational upgrades. By October 2025, they’ll also need to send instant payments, tackling challenges like payee verification, bulk payments, and liquidity management.

This regulation is expected to boost merchant adoption by easing infrastructure costs and cutting through cross-border complexity. Europe’s growing demand for a widely accessible instant payments solution signals a big opportunity. Globally, A2A instant payment systems are gaining ground and proving highly effective.

Together, the IPR and solutions like Wero create a major opportunity to meet the growing demand for instant payments with broad reach across Europe, mirroring the global trend where A2A instant payment systems are rapidly evolving and achieving strong success in enhancing payment efficiency and merchant liquidity.

Breaking barriers, building momentum

As global commerce grows, so does the need for faster, more integrated financial solutions. Yet challenges still hinder cross-border real-time payments—fragmented regulations, limited interoperability, restricted FX access, and rising cyber and fraud risks.

Infrastructure modernisation is addressing these gaps. ISO 20022 offers a standardised messaging format to improve cross-border data quality. Projects like BIS’s Project Nexus aim to connect domestic real-time payment systems via a central hub, reducing the need for multiple bilateral integrations and enabling seamless, cost-effective cross-border transactions.

Cross-border payments are an incredibly important part of the global payments landscape, associated with a revenue pool of approximately USD 280 billion. However, the market has for a long time been plagued by multiple customer pain points, ranging from price to speed of settlement. Settlement speed is particularly important for some customer use cases, including P2P remittances. Consequently, we have seen this becoming an area of increasing focus for players globally, including Swift and the BIS, as well as a number of private sector initiatives.

Overall, the outlook for cross-border real-time payments is promising, supported by technological advancements, regulatory support, and evolving consumer expectations—particularly in markets with domestic real-time payments. Therefore, we are seeing a real effort to modernise payment infrastructures, and some of the most interesting ones include:

- A number of bilateral and multilateral initiatives to connect domestic instant payment schemes. For instance, the successful linkage of UPI from India and Singapore's PayNow platform, albeit for very low-value payments for now, is incredibly exciting, as is the proof-of-concept connection between Malaysia's Real-Time Retail Payments Platform (RPP) and Singapore's Fast and Secure Transfers (Fast) payment system under Project Nexus.
- In parallel, we have seen a number of private sector players building out new networks that they provide as a service, including traditional players like HSBC and DBS, as well as newer players like Wise.
- In addition, there are now multiple players launching attempts to facilitate real-time cross-border payments, leveraging public (e.g., USDC, USDT) and private (e.g., XRP, PYUSD) stablecoins, which are gaining increasing traction among fintechs and other challengers, and may over time even be used by banks.

However, while rail innovation continues to capture much of the attention, customers are more focused on pricing and overall experience. The real winners will be those who can deliver exceptional customer experiences—regardless of the underlying rail—especially when tailored to specific customer niches and use cases."

Uzayr Jeenah
Partner at McKinsey

Public-private collaboration is key. The FSB and BIS are working with the private sector to improve data standards, foster interoperability, and connect domestic systems. New regulations and service-level agreements are boosting transparency, efficiency, and trust.

Thriving real-time payment ecosystems share traits: collaboration among financial players, government, and fintechs; strong merchant incentives; and open platforms that support smaller players. Adoption grows when real-time systems tie into user-friendly, popular use cases. In Asia, especially, cross-border ambitions are turning real-time payments from domestic tools into global infrastructure.

Future outlook

As digital transformation continues to reshape financial services, businesses will need to adapt by integrating real-time payment solutions into their operations. With strong market momentum and increasing global adoption, real-time payments are set to become a cornerstone of the modern B2B payments ecosystem.

The future of real-time payments: How A2A reshapes the financial landscape

Craig Ramsey, Head of Real-Time & A2A Payments at ACI, discusses compliance and innovation in the context of how A2A payments transform finance.

Could you please provide a brief explanation of A2A payments and their benefits in comparison to card payments?

A2A payments have gone by many names over the years, including wholesale and corporate payments, though these terms don't fully capture their broad scope. A2A payments encompass four key payment types that facilitate direct money transfers between accounts: wire transfers (or RTGS internationally), ACH, instant payments, and cross-border transactions.

Each of these payment types serves various use cases, including P2P, B2B, C2B, and even government payments—highlighted recently by the U.S. government's push to expand A2A adoption. Cross-border payments are traditionally handled via Swift and correspondent banking, though new alternatives are emerging. Wire transfers operate through systems like Fedwire and CHIPS in the U.S., Target2 in Europe, and CHAPS in the U.K., with most countries have their own domestic RTGS infrastructure. ACH payments include networks such as SEPA in Europe and FedACH or EPN in the U.S.

Instant payments, the newest category now leading modernisation, are also referred to as faster payments, real-time payments, or immediate payments. This system enables 24/7, low-cost, instant clearing and settlement, eliminating float and ensuring immediate availability of funds. Unlike card transactions, where pending payments may take days to reflect, instant payments provide real-time balance updates, making them particularly valuable for individuals managing liquidity constraints.

Ultimately, A2A payments eliminate intermediaries, reducing delays and inefficiencies while giving both senders and recipients immediate access to their funds.

As A2A payments and increased digitisation reshape the payments landscape, how is ACI Worldwide supporting FIs in navigating regulatory complexities, ensuring compliance, and minimising risk—particularly in cross-border transactions where security, fraud prevention, and cost efficiency are critical?

ACI processes around USD 5 trillion in A2A payments every day—yes, trillion, not billion. This includes a significant share of wire transactions in the U.S. as well as CHAPS in the U.K. and Target2 in Europe. As each payment network introduces new compliance requirements, often on an annual basis, ACI ensures that banks remain compliant by providing a fully maintained and updated gateway. Instead of managing these updates independently, which can be costly and complex, banks benefit from ACI's centralised approach. A clear example is the global transition to ISO 20022, a regulatory shift that has required banks to invest millions. By handling these updates centrally, ACI reduces the burden and cost for its customers.

Regarding fraud in international payments, the risks are not unique to cross-border transactions. Fraud affects all payment types, whether card-based, domestic, or international A2A transactions. ACI integrates fraud prevention measures into its solutions, allowing banks to incorporate third-party protections. Detecting fraud involves multiple layers of security, starting with transaction scoring, which analyses payment patterns to flag suspicious activity. Anti-money laundering efforts rely on monitoring broader transaction flows rather than isolated payments, helping to identify illicit activities. Additionally, sanctions screening, commonly known as OFAC screening in the U.S., ensures that payments comply with global regulatory lists and do not involve restricted individuals or entities.

Sanctions screening is a particularly crucial component of international payments, and ACI's built-in compliance mechanisms help banks navigate these requirements efficiently.

With economies becoming increasingly reliant on digital payments, how can banks ensure availability, resilience, and security in their payments infrastructure? What role do factors like scalability, uptime, and fraud prevention play in meeting customer expectations?

Customer expectations for payments have evolved significantly, both in the consumer and business spaces. Today, people expect payments to be instant, fully trackable, and transparent. They want to know exactly when a transaction will reach the beneficiary, how much it will cost, and where it is in the process. These demands have transformed payments from a traditional batch process into a real-time, always-on system. Even in cases where payment networks do not operate 24/7, the expectation remains the same—immediacy, visibility, and certainty. Given how seamlessly technology works in other aspects of life, it's only natural that payments should follow suit.

However, these rising expectations place immense pressure on banking systems, many of which were built decades ago. Some of these legacy systems still rely on batch-based architectures designed for a different era of payments processing. Even systems developed just 10 years ago often struggle to meet modern demands. The shift to cloud-native technology has introduced a more flexible and scalable approach, allowing for improved disaster recovery, elastic processing, and higher availability standards.

Yet, simply moving an old system to the cloud doesn't magically modernise it. True cloud-native solutions are purpose-built to meet the demands of today's real-time payments landscape. This shift also enables a reimagining of payment processing—not just adapting old models to new infrastructure, but fundamentally redesigning how payments operate to support the next two decades of innovation.

Rising payments fraud: Navigating APP scams, real-time risks, and the AI threat landscape

The evolving regulatory landscape calls for a transformative approach to fraud prevention—one that strikes the right balance between accountability, real-time compliance, and a seamless customer experience. As the fraud landscape continues to shift, it brings both new challenges and opportunities for merchants, FIs, and consumers.

While FIs grapple with regulatory changes, speed of settlement, and advanced fraud schemes, merchants face their own distinct set of vulnerabilities tied to the rapid expansion of eCommerce. According to the latest Global Payments and Fraud Report by MRC, a significant share of merchants are dealing with top threats such as real-time payments fraud, refund and policy abuse, phishing, card testing, and first-party misuse. These issues lead to chargebacks, increased payment processing fees, and operational disruptions. The financial and reputational costs can strain businesses, with some facing account downgrades or even terminations, further impacting their bottom line and long-term stability.

Real-time payments are growing at an exponential rate, but with faster payments comes the risk of faster fraud. According to the MRC report, merchants need to invest in fraud management by monitoring the entire buying cycle, exploring AI tools, and improving data usage for more accurate fraud prevention. Banks should support merchants by facilitating real-time payments adoption, offering solutions to combat refund/policy abuse and first-party misuse, and providing resources to enhance authorisation rates and payment security while staying updated on evolving fraud tactics.

Of particular note are APP scams, which rely on manipulating victims into transferring funds willingly and are also expected to surge. According to ACI Worldwide, these scams could cost real-time payment markets an estimated USD 7.6 billion by 2028. APP fraud losses through real-time payments (as a percentage of overall APP fraud losses) are predicted to increase from 63% in 2023 to 80% in 2028, an increase of more than USD 3.3 billion in value.

> In 2025, MRC sees the payments landscape defined by two accelerating forces: the rapid growth and globalisation of real-time payments and the rise of agentic AI, transforming eCommerce. With speed and intelligence come new weaknesses, and we can already see from the MRC Annual Global Payments and Fraud Report that fraud and scams are growing. The solutions lie not just in isolated defence systems, but in deep, sustained collaboration.
>
> Fragmented intelligence enables fraudsters to exploit vulnerabilities. Cross-sector information sharing and collaboration are critical. MRC focuses on effective public-private collaboration. We see, strategically, that businesses that embed collaborative intelligence into their risk and payments strategies gain a trust and performance edge.
>
> Challenges persist, from data privacy and regulatory complexities to the commercial incentives needed to drive sustained cooperation. Data-sharing innovations are also part of the solution, ensuring rich data is passed in authorisation streams, increasing approvals and minimising false declines, helping avoid a poor customer experience.
>
> Regulators are evolving to support this shift, creating space for innovation through shared standards and stakeholder engagement. Cross-industry collaboration is no longer optional—it is necessary. To build a more secure, resilient, and intelligent payments ecosystem, we must work collectively, think globally, and act quickly.
>
> **Úna Dillon**
> VP Global Expansion & Advocacy at Merchant Risk Council

Fraud threats are multifaceted and affect all stakeholders in the payments ecosystem:

- **APP:** APP scams exploit individuals' trust by manipulating them into making voluntary fund transfers, making detection difficult. These scams are growing rapidly with the adoption of real-time payments, offering scammers the chance to quickly divert funds.
- **Real-time payments fraud:** Real-time payments fraud occurs when a fraudster tricks a customer into instantly transferring funds, often by impersonating a legitimate merchant through fake invoices or websites. Because real-time payments settle within seconds and are irreversible, there's no opportunity to intercept or reverse the transaction. Traditional fraud tools may not detect these scams in time, and merchants can suffer brand damage and customer trust issues if their name is used fraudulently.

AI-fuelled synthetic identity fraud: Fraudsters are increasingly leveraging AI to generate synthetic identities on a massive scale, blending genuine and fabricated information to open accounts and commit fraud. Scammers use AI not only to automate the creation of these identities but also to enhance trust through highly effective social engineering techniques. AI-driven bots and scripts make it faster and harder to detect fraudulent activity, pushing synthetic identity fraud to new, more dangerous levels. In the first half of 2024, synthetic identity fraud rose by 26%.

- **Refund/policy abuse:** When customers deliberately exploit a business's return or refund policies to get money or products they are not entitled to—such as returning used or damaged items, claiming items never arrived, or repeatedly abusing lenient policies.
- **Phishing attacks:** Fraudulent attempts to trick individuals into revealing sensitive information like passwords or credit card details, often through fake emails, websites, or messages that impersonate trusted entities.
- **First-party misuse:** When legitimate customers intentionally misuse services or products for personal gain, such as using a product temporarily and then returning it (wardrobing) or abusing promotional offers and return policies without involving stolen payment data.
- **Card testing:** A fraud tactic where criminals use stolen or guessed credit card numbers to make small transactions to verify which cards are active and valid before committing larger fraudulent purchases.
- **Evolving scam tactics:** In 2025, fraudsters are evolving rapidly, using social media to find targets and employing tactics like deepfakes, phishing, and brand impersonation to bypass security and commit scams. They exploit new technologies and platforms, making vigilance essential.

Strategies for combating fraud

To effectively fight this rising tide, both FIs and merchants need a collaborative, multilayered fraud prevention strategy that blends technology, education, and shared intelligence.

FIs must collaborate and share fraud intelligence to stay ahead of emerging threats. AI-driven fraud management systems play a vital role by analysing real-time transaction data, detecting anomalies, and automating fraud protection, enabling quicker responses across sectors. Strengthening real-time fraud detection with AI and ML allows for dynamic risk assessments and early identification of fraud patterns.

Sharing intelligence between FIs, payment processors, and merchants can strengthen defences against emerging threats. Initiatives like federated machine learning (FML) and real-time network intelligence improve the detection of synthetic identities and suspicious transactions. FML allows different institutions to work together to detect fraud without sharing sensitive customer data, while real-time network intelligence helps detect unusual transactions quickly and adjust risk levels as new threats emerge.

Merchants, too, have an important role to play. Tools like 3D Secure (3DS) authentication, device fingerprinting, and advanced chargeback management systems help mitigate eCommerce-specific fraud. Unified KYC/AML workflows—especially those using biometrics and ISO 20022 data—can streamline onboarding while improving fraud detection. Pre-payment screening and Confirmation of Payee (CoP) solutions are critical to intercepting APP scams before they occur.

Customer education is crucial in preventing fraud, as informing users about common scams can reduce risks. Data analytics and predictive modelling further help detect anomalies and anticipate future fraud trends. Stricter KYC procedures are essential to prevent fraudulent identities from infiltrating platforms.

By combining AI-driven detection, smarter data analysis, collaboration across sectors, and ongoing customer education, merchants and FIs can create a more resilient defence against fraud. In a world of faster payments and evolving threats, the key is to stay just one step ahead.

The role of regulation

Regulators across the globe are intensifying their focus on accountability and liability allocation to protect customers and prevent fraud. FIs and merchants are under pressure to leverage technology, share data, and participate in industry-wide fraud intelligence initiatives. Compliance with government mandates and the implementation of robust fraud prevention systems are now essential for all players in the payments ecosystem.

Proactive modernisation not only ensures compliance but can also serve as a competitive differentiator, enabling institutions and merchants to build trust and attract customers in a security-conscious market.

The cost of inaction

Institutions that fail to modernise their fraud prevention systems risk facing significant consequences:

- **Unlimited fines:** Under the U.K.'s Economic Crime and Corporate Transparency Act, banks could face unlimited fines for failing to implement adequate fraud prevention controls.
- **Reputational damage:** FIs and merchants that do not adequately protect customers risk long-term reputational harm. Loss of trust can lead to customer attrition and negative brand perception.
- **Legal consequences:** Governments worldwide have established strict laws and penalties to deter money laundering and ensure transparency in financial transactions. Non-compliance with evolving regulatory mandates can result in lawsuits or legal actions, which can further escalate financial and reputational damage. Failure to comply with regulations like AML and KYC can also lead to increased scrutiny from regulators. Entities found in violation of AML regulations may face hefty fines, civil or criminal charges, and reputational damage.
- **Competitive disadvantage:** FIs and merchants that lag in adopting advanced fraud prevention technologies risk falling behind more innovative competitors. This can hinder growth, limit partnerships, and reduce customer acquisition as consumers and business partners increasingly prioritise security.

Future outlook: Balancing security and customer experience

As fraud evolves, FIs and merchants must strike a balance: strong security without sacrificing customer experience.

Frictionless onboarding is key—too much friction drives cart abandonment and customer churn. APP scams and rising fraud risks also erode trust, pushing users to look elsewhere.

AI and ML enable real-time fraud detection with minimal friction. Tools like dynamic profiling, sanctions screening, and CoP help stop threats before they hit.

Collaboration matters. Sharing intelligence across FIs, merchants, and processors strengthens defences and speeds response.

Advanced technology—like FML, biometrics, and enhanced KYC/AML workflows—helps spot fraud fast while keeping onboarding smooth.

The goal: secure, compliant, and seamless payments that protect businesses and their customers.

AI-powered fraud prevention: Tackling identity theft, payments fraud, and scams in real time

Cleber Martins, Head of Payments Intelligence & Risk Solutions at ACI Worldwide, explains how AI and ML enhance fraud detection by analysing real-time data and enabling adaptive, collaborative intelligence.

Given the increasing sophistication of cybercrime and the significant financial losses due to fraud, how can AI and ML solutions enhance fraud detection and prevention for FIs, especially in identifying and mitigating emerging threats like identity theft, payment fraud, and scams across various channels and payment methods?

Identity theft, scams, and payments fraud are closely linked, with criminals often targeting identities to create accounts for moving and controlling funds. They exploit new payment methods to access cash more quickly, bypassing traditional steps like selling products on the black market, which is common in eCommerce fraud.

This issue is escalating as criminals find new ways to access and move funds. Over the past 20 years, banks have implemented robust security measures to ensure only account owners can initiate transactions, keeping systems secure. However, scams—especially APP fraud—have changed the landscape. In APP fraud, criminals manipulate customers into making payments themselves, bypassing the bank's security controls. As the victim believes the payment is legitimate, fraud detection becomes increasingly difficult.

This is where AI becomes crucial. Fraud detection requires analysing massive amounts of data in real time—something beyond human capability. Criminals often use social engineering tactics, such as creating a sense of urgency or exploiting inherited trust by posing as someone the victim knows. AI can detect subtle behavioural signals, like a rushed transaction, that indicate fraud, allowing banks to intervene in real time. AI advancements are necessary to identify such patterns quickly—a task that would be difficult for a human observer to catch.

Without advanced AI, banks face challenges such as blocking transactions based on recipient or amount, which can frustrate legitimate customers. As the demand for faster and more reliable payment methods grows, outdated fraud detection systems risk alienating customers. Meanwhile, criminals also use AI to scale their operations, targeting vulnerable individuals and creating deepfake voices to impersonate loved ones, making scams harder to detect.

This has created a technological arms race, where criminals can deploy advanced AI tools, and banks must invest in real-time, adaptive AI solutions. Relying solely on historical data is no longer enough. The next generation of AI will enable real-time, collective learning, allowing FIs to share insights and adapt to emerging threats faster.

With the rapid rise of immediate payments and scams, the financial and legal implications are high. The future of fraud prevention lies in real-time, adaptive AI systems that protect customers and keep pace with evolving threats.

Considering the complexities of global payment ecosystems and the need for real-time fraud detection, what strategies and solutions can help banks and payment processors effectively analyse large volumes of transactional and behavioural data, detect anomalies, and prevent fraud in cross-border payments, while complying with diverse regulatory requirements and ensuring a seamless customer experience?

This question is crucial because it highlights one of the biggest challenges we'll face as we move into this new era of collaboration. As I mentioned earlier, the key is leveraging technology that allows banks to learn together, without compromising their customers, data, or internal strategies. Rather than centralising all the data in one place, the focus should be on bringing the learning to where the problem exists, instead of trying to collect and analyse everything in a single location. Given the complexity of modern financial fraud, a decentralised, real-time approach is essential.

From a technology perspective, many of these new payment methods are built on the ISO 20022 protocol—a highly data-centric payment messaging standard. Unlike traditional payment systems, ISO 20022 allows transactions to carry much more information than just the sender, receiver, and transaction amount. This protocol can embed AI-driven signals—intelligence collected at the point of transaction initiation—into the payment itself, in a format that is not human-readable, almost like a digital DNA.

This advancement allows FIs to exchange intelligence in real-time without compromising customer privacy or revealing their internal fraud prevention strategies. It fosters an ecosystem where banks can collectively learn from each other, strengthening fraud detection across the board.

The future of payments and fraud prevention lies in real-time intelligence exchange. AI systems must be able to:

1. **Transport and consume real-time fraud signals** embedded in payments.
2. **Correlate these signals** with existing data from the initiating bank, central payment infrastructures, and the receiving institution.

Central payment infrastructures, which act as intermediaries for new payment methods, play a critical role in this ecosystem. They have a unique, independent view of transactions flowing through the system. By combining intelligence from:

- The initiating bank (which sees customer behaviour and account activity),
- The central infrastructure (which monitors transaction flow at a broader scale), and
- The receiving institution (which has insight into account ownership and potential fraudulent activity on the other end),

these three entities can work together to make precise, real-time decisions about potential fraud.

One of the biggest challenges in combating scams—especially APP fraud—is that criminals have full visibility into the entire fraud scheme, while FIs only see fragments of the process.

Criminals understand:

- **Who they are attacking** and how to manipulate them.
- **Which bank products and processes** they need to exploit to bypass security controls.
- **How the transaction will flow** and what weaknesses exist along the way.
- **How to retrieve and launder the stolen funds**, whether through cash withdrawals, cryptocurrency, or other means.

Right now, FIs and payment networks are playing catch-up because they only see pieces of the puzzle, whereas criminals see the entire picture. However, real-time intelligence sharing through embedded fraud signals can change that.

By combining intelligence from multiple sources, banks and payment networks can gain greater visibility than the criminals themselves, enabling them to detect and block fraudulent transactions faster than ever before. When fraudsters encounter a system that predictively blocks their schemes in real time, they're forced to abandon those tactics and look elsewhere.

This is the future of fraud prevention—one where AI-driven, real-time collaboration makes financial ecosystems more resilient than ever.

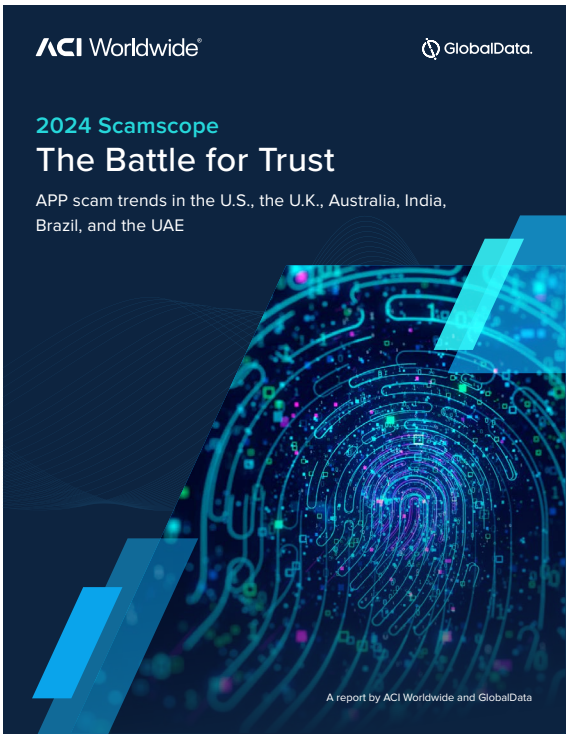
Given that various reports estimate the global cost of fraud to be in the trillions of dollars annually, impacting GDP, household finances, and even fuelling other crimes, how does ACI Worldwide help its clients quantify the economic impact of fraud reduction through their services? Additionally, what innovative approaches can be used to further minimise the broader societal and economic consequences of fraud on a global scale?

Fraud is a major global issue impacting trust, FIs, and economies. ACI Worldwide, a leader in payments for 50 years, has driven real-time, account-to-account payments that are faster, more cost-effective, and enhance financial inclusion, positively impacting GDP by putting money back into the economy. Many governments support next-generation payment systems for these benefits.

To help the industry understand fraud reduction's economic benefits, ACI collaborates with specialists to produce research on global trends in real-time payments. These reports also highlight fraud evolution and criminals adapting to exploit new methods, with ACI's Scamscope report tracking scams' rising impact on the financial ecosystem.

ACI works with FIs globally, leveraging cross-market intelligence to help partners stay ahead of emerging fraud tactics. Collaboration and AI-driven intelligence sharing are key to combating fraud. ACI empowers real-time fraud detection by fostering seamless collaboration between institutions, allowing them to stop fraud before it spreads. AI-powered models integrate localised fraud prevention with global intelligence, continuously learning and adapting to ensure swift, effective responses.

By combining expertise, AI-driven intelligence, and global collaboration, ACI Worldwide leads the fight against fraud, helping FIs stay ahead of emerging threats and strengthening the financial system.



Tokenization: The future of secure and intelligent digital payments

Card networks (Visa, Mastercard, American Express, and Discover) are now pushing for the adoption of tokenization—a process where sensitive payment data is replaced with a unique numeric sequence called a token. This shift enhances security by ensuring that actual payment details are never exposed during transactions.

The strategic benefits of tokenization

Online shopping has evolved significantly since the 1990s, but with it came a rise in fraud. As customers stored card details across multiple merchants, opportunities for fraud increased, making merchants' databases prime targets for hackers. A 2023 study projected that merchant losses from online payment fraud will exceed USD 91 billion by 2028, underscoring the need for stronger security measures.

To address this, card networks are focusing on network tokenization, Click to Pay, and passkeys, which offer security, efficiency, and compliance benefits.

> “Tokenization is not just a technological advancement; it's a fundamental shift in how businesses and industries safeguard sensitive information. By replacing critical data with unique tokens, we significantly reduce the risk of data breaches and fraud. This enhanced security is crucial for maintaining customer trust and ensuring seamless transactions. As digital payments continue to evolve, prioritising tokenization is essential for any business looking to thrive. Tokenization benefits the entire ecosystem by enhancing security and improving transaction approval rates. This creates a win-win scenario for merchants, consumers, and issuers, making the digital economy safer and more efficient for everyone.”
>
> **Brice van de Walle**
> Executive Vice President, Core Payments Europe
> Mastercard

Network tokenization: Boosting security and efficiency

Network tokenization enhances payment card data protection for remote commerce and wallet-based transactions. Introduced with Apple Pay and major payment networks, it's now an industry standard accessible to all participants.

Network tokenization replaces a card's Primary Account Number (PAN) with a unique token from card networks like Visa, Mastercard, Discover, or American Express. Unlike processor-specific tokenization, network tokens are interoperable and dynamically updated in real time, with each transaction secured by a cryptogram.

A Juniper Research study projects global network tokenized transactions to double by 2029, growing from 283 billion in 2025 to 574 billion, with revenues rising from USD 4.1 billion to USD 8.9 billion. This growth reflects the technology's role in enhancing security, reducing fraud, and improving approval rates, particularly in eCommerce, mobile payments, and Internet of Things (IoT) transactions, while ensuring PCI DSS compliance.

Visa reports that network tokens reduce fraud by 30% and boost authorisation rates by 2-4.6%, highlighting tokenization's role in improving security and transaction approval rates across eCommerce, mobile payments, and IoT.

Key benefits of network tokenization include:

- **Fraud reduction:** Tokens hide PANs, preventing fraud, while passkeys enhance security by eliminating credential theft.
- **Higher authorisation rates:** Tokenized transactions and built-in lifecycle management reduce false declines and boost approval rates by up to three percentage points, especially in subscription models.
- **Automatic updates:** Automatically updates expired or replaced cards, reducing declines and PCI scope.
- **Frictionless checkouts:** Enables one-click payments, reducing cart abandonment and improving the checkout experience.
- **Simplified compliance:** Eases PCI compliance and lowers interchange fees, making transactions more cost effective.
- **Improved customer experience:** Supports smooth recurring payments, fewer declines, and builds trust in payment security.

Applications in cloud-based payment ecosystems

Network tokenization is a transformative technology that plays a vital role in modern cloud-based payment orchestration platforms, especially those handling complex, multichannel transactions. By leveraging network tokenization, these platforms can:

- **Optimise routing decisions:** Dynamic updates to payment credentials enable real-time routing optimisation, ensuring faster and more efficient transaction processing.
- **Ensure scalability and security:** Tokenization helps platforms scale seamlessly, while maintaining robust security across distributed systems, safeguarding both transaction data and customer information.
- **Facilitate reliable recurring payments:** By supporting subscription-based business models, network tokenization improves the reliability of recurring payments, ensuring continuous billing without disruptions.

How leading merchants are adapting: Future-proofing payments with network tokenization

Forward-looking merchants aren't waiting. They're following a clear playbook:

1. **Pursue acquirer-agnostic tokens:** This ensures flexibility and protects against outages or suboptimal approval rates.
2. **Optimise for approval uplift:** Higher authorisation rates and fewer declines improve customer experience and revenue.
3. **Implement smart failovers:** Advanced merchants own their Transaction Request ID, use orchestration platforms, and maintain universal token backups to reduce failed transactions.
4. **Future-proof the payments stack:** Combining network tokens with biometric authentication, Click to Pay, and Tap to Pay capabilities helps merchants stay ahead of evolving standards.

To stay ahead, merchants should embrace network tokenization now, before it becomes mandatory. Early adoption not only helps reduce fraud but also improves transaction success rates and provides greater control over payment flows. By leveraging a flexible, agnostic orchestration layer, merchants can maintain data portability, avoid vendor lock-in, and stay agile in an evolving payments landscape. They should also take advantage of available network tokenization incentives, ensure that their acquirers support network token processing, and use orchestration platforms that enable token portability. Developing fallback strategies is also essential to prevent payment disruptions and maintain continuity.

Success in this space also depends on close collaboration with acquirers, a willingness to experiment with emerging payment technologies, and a proactive approach to system upgrades. Merchants that invest in these capabilities now will be well positioned to optimise performance, protect their operations, and deliver a smoother, more secure customer experience in an increasingly digital economy.

X-Pay and Click to Pay: Increasing conversion and reducing declines

Apple Pay and Google Pay (often referred to as X-Pay solutions) are leading mobile wallets that use tokenization and encryption to protect cardholder data. When a user pays with these wallets, the actual card number is never shared with the merchant. Instead, a unique token is generated for each transaction, ensuring that sensitive card information remains secure reducing the risk of fraud. Both platforms also leverage biometric authentication, such as fingerprint or facial recognition, adding an extra layer of security and convenience for consumers.

Recognising the value of tokenization, Visa and Mastercard are actively promoting their own universal checkout solution: Click to Pay. Unlike device-specific wallets, Click to Pay is based on EMV Secure Remote Commerce standards and is designed to provide a unified, scheme-agnostic, and device-agnostic online payment experience. This means that consumers can use Click to Pay across different devices, browsers, and merchants without needing a specific app or hardware.

Click to Pay streamlines online checkout by removing the need to manually enter card details, reducing friction and cart abandonment. It uses network tokenization to improve approval rates and minimise declines from outdated card info. By replacing sensitive card data with secure tokens, it enhances security and eases PCI compliance.

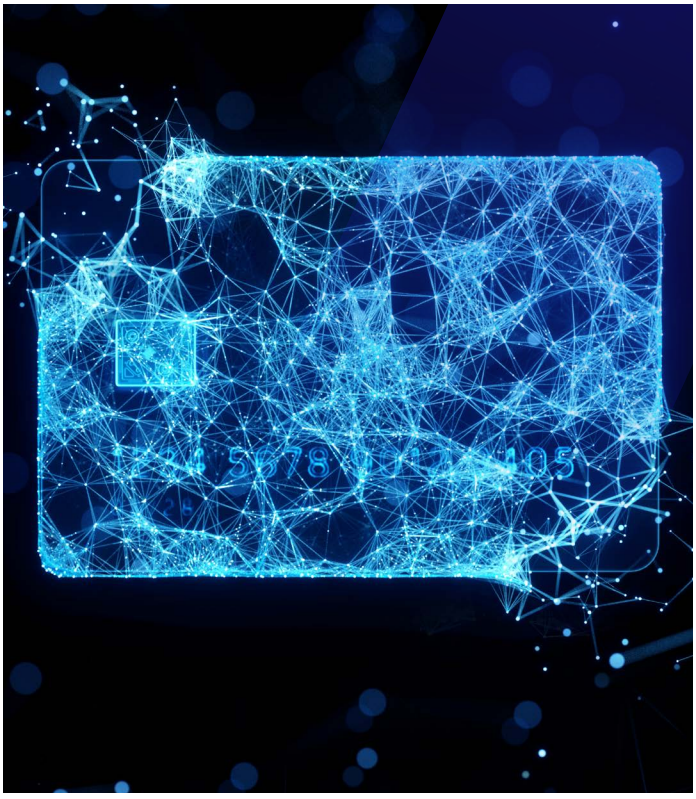
Passkeys: Moving toward a passwordless future

A trusted identity is the backbone of the digital economy, allowing people to interact securely and confidently, whenever and wherever they choose. Biometrics, ML, and identity insights are already enhancing authentication throughout the customer journey. The rise of passkeys is accelerating this shift, with adoption expected to grow significantly in 2025.

Passkeys offer passwordless authentication by using biometrics, such as Face ID or fingerprint recognition, or secure device PINs. Integrated with Click to Pay, passkeys replace traditional one-time passwords and 3DS flows, helping reduce friction during checkout while still meeting Strong Customer Authentication requirements under PSD2/3 regulations. By providing phishing-resistant security, passkeys further strengthen trust in tokenized transactions, enhancing both the user experience and the overall integrity of digital payments.

Passkeys, powered by biometrics, eliminate passwords and improve payment security. Benefits include:

- **Enhanced security:** Prevents phishing and fraud by using unique biometric data.
- **Faster checkout:** Simplifies login and payment, improving speed and user experience.
- **Improved trust:** Eliminates the risks associated with password theft, ensuring safer transactions.



How tokenization is powering the future of intelligent commerce

Recently, Visa and Mastercard have launched AI-powered shopping solutions that allow AI agents to shop and make purchases on behalf of consumers based on their preferences. Visa's Intelligent Commerce and Mastercard's Agent Pay integrate AI with payment systems to create personalised, secure, and convenient shopping experiences. These AI agents can curate product selections and complete transactions, leveraging collaborations with tech leaders like Microsoft, IBM, OpenAI, and others.

This move follows similar initiatives by PayPal and Amazon, signalling a broader industry shift toward AI-driven, agentic commerce that simplifies and personalises online shopping. With agentic commerce, AI agents not only assist shoppers but autonomously complete purchases on their behalf.

Central to this innovation is tokenization, which gives AI agents unique, controlled payment tokens linked to consumers' cards, ensuring safety and spending limits. Visa and Mastercard collaborate with AI leaders like OpenAI and Microsoft to embed payment functions into chatbots, while PayPal offers developer tools for direct AI integration via APIs.

This shift promises to transform retail by delivering personalised, intent-driven shopping experiences, reducing returns, and saving consumers' time. However, success hinges on building consumer trust, ensuring transparency, and implementing safeguards that keep users in control of payments. Retailers must adapt by providing real-time data to AI agents to stay competitive in this emerging landscape.

A strong start, but more work to be done

While network tokenization is gaining traction globally as a key innovation in payment security, its adoption remains uneven, particularly across European markets.

Adoption of network tokens has been relatively slow, with varying experiences across different markets. In the U.S. market, adoption rates are higher, driven largely by the prevalence of card transactions. Stakeholders across the ecosystem have prioritised the implementation of network tokenization technologies, with strong advocacy from merchants playing a key role in driving progress.

In contrast, Europe is experiencing slower adoption rates. Issuers and acquirers in the region face busy roadmaps and legacy infrastructure challenges, and network tokenization is not currently viewed as a top priority. Despite the clear benefits of the technology, the lack of regulatory mandates has also contributed to its slow adoption.

Visa and Mastercard push for a tokenized, card-free eCommerce future

Visa and Mastercard have agreed to speed up the adoption of secure payment tokens—they are pushing for a tokenized, card-free eCommerce future, reshaping online payment security with network tokenization and Click to Pay. By integrating these with passkeys, they're boosting security, cutting costs, and simplifying checkout, while ensuring global scalability and compliance. This collaboration allows each network to request tokenized payment credentials from the other's digital wallet platforms, enabling cross-network tokenization support. It's a strong move toward the future of seamless, secure payments.

According to Visa, network tokens are proving highly effective at enhancing both security and transaction performance in digital payments. Network tokens help reduce fraud, offering significant protection for both merchants and consumers. Mastercard reports that network tokenization reduces fraud by up to 50% compared to traditional credit card transactions, while Visa reports a fraud reduction of up to 34% on their platform.

Introduced in 2014, Mastercard's tokenization service today secures 25% of all eCommerce transactions globally, with adoption accelerating 50% year-over-year. Mastercard's goal is to phase out manual card entry in eCommerce by 2030, with a vision for 100% eCommerce tokenization in Europe by the end of the decade. To achieve this goal, Mastercard is combining tokenization with Click to Pay and biometric passkeys to phase out manual card entry for online payments. Both technologies work together to make online transactions safer and easier for consumers and merchants. This aligns with a broader global commitment to eliminating manual card entry, improving security, and making online transactions safer and more accessible for all.

The drive to 100% eCommerce tokenization by 2030 promises a safer, faster, and more seamless online shopping experience that benefits all stakeholders by reducing fraud, simplifying checkout, and enabling new payment innovations.

For merchants, tokenization means better security and lower fraud risk by replacing sensitive card data with secure tokens. This helps prevent data breaches and builds customer trust. It also improves the checkout experience with one-click payments and automatic card updates, which reduce cart abandonment and boost approval rates—great for subscriptions and repeat purchases. On the backend, merchants benefit from lower costs, easier PCI compliance, and support for secure payments across online, in-app, and in-store channels. Tokenized payments also provide better data for personalised marketing and loyalty programs.

For FIs, tokenization reduces fraud losses, chargebacks, and the costs of investigations. It also supports regulatory compliance with evolving standards like AML and PCI DSS. Higher approval rates and fewer false declines lead to more transactions and revenue. The partnership between Mastercard and Visa improves how tokenized credentials are shared across wallets and platforms, making operations smoother and preparing FIs for future technologies like biometrics and digital wallets.

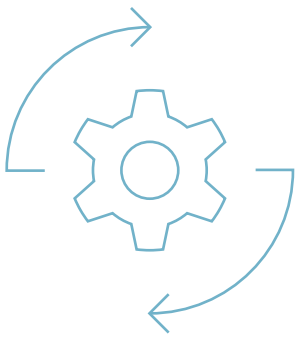
Navigating the future of payments: Trends, challenges, and opportunities for banks

From payments growth to modernisation, bank execs are rethinking strategy. **Phil Bruno**, Chief Strategy & Growth Officer at ACI, discusses how they can stay competitive in a shifting landscape.

With rising regulatory pressures, cybersecurity risks, competitive threats, and the rapid pace of digital transformation, what are the biggest concerns keeping bank executives up at night, and how can they address them?

Right now, one of their biggest concerns is the uncertainty surrounding the future. Bank executives are trying to navigate questions about the global economy—where interest rates are headed, whether they'll rise or fall, and which sectors will drive growth. This helps them determine where to lend and invest.

Another major priority is determining the best path for growth. They are evaluating various parts of their business—such as commercial lending, consumer banking, credit cards, and small business—to identify the most effective investment strategies for the future.



How is ACI Worldwide helping banks modernise their payments infrastructure to enhance efficiency, interoperability, and cost reduction across all payment types?

Let me start by looking at both the banking and customer perspectives as they approach the modernisation of their tech stack. The era of large-scale 'rip and replace' core banking overhauls is coming to an end. Many banks have faced challenges, false starts, and even failures when trying to modernise from a core-first strategy. As a result, we're now seeing a shift toward a more modular and strategic modernisation approach.

Additionally, tech budgets have declined compared to two years ago, forcing banks to be more deliberate about their investments. This has led to a few different modernisation strategies.

One approach is what I'll call a 'hollow out the core' strategy—keeping the existing core system but reducing its role to a system of record while modernising the surrounding infrastructure. This includes upgrading channel software, risk and fraud management, product catalogues, pricing, and underwriting.

A key priority in this modernisation effort is payments. Banks are focusing on revamping their payments stack across various payment types, particularly in commercial payments such as wire transfers, ACH, and instant payments—especially in North America, where adoption is growing. They are also modernising cross-border payments through Swift, as well as upgrading orchestration and switching capabilities for card-based payments, including credit, debit, and ATM transactions.

At ACI, we are supporting this transformation through ACI Connetic®, our cloud-native payments hub and orchestration layer. ACI Connetic enables banks to modernise in a modular way, allowing them to adopt a common architecture that fits their needs while ensuring scalability and flexibility across all payment types.

As banks centralise and streamline their payment capabilities, what new business models are emerging? How do innovations like payments insurance, improved payment visibility and routing, and lower merchant fees through A2A payments create new opportunities?

Great question. Traditionally, banks have approached modernisation primarily to cut costs, focusing on reducing processing expenses, optimising interchange fees, and improving operational efficiency. While cost management is still important, it has shifted to a lower priority. Now, banks view modernisation through a broader lens, starting with how an improved payments stack can drive revenue growth, followed by improving the customer experience, and finally, increasing efficiency and reducing costs.

Another critical factor in this shift is risk, regulatory compliance, and reporting. For some institutions facing significant regulatory pressure, this can be the top priority, while for others, it remains important but ranks lower in their strategic focus.

When it comes to innovation, the increasing digitisation of payments and advancements in payments infrastructure are unlocking new opportunities for value-added services, which are becoming a substantial revenue driver for banks. On the corporate side, a modernised payments stack that integrates various payment types allows businesses to better manage financial exposure. Instead of relying on traditional 30-, 60-, or 90-day receivable aging, companies can dynamically assess and qualify receivables in real time. Additionally, improved straight-through processing enhances liquidity management, ensuring a more seamless cash flow.

As the entire accounts receivable and payables ecosystem becomes digitised, banks can offer more comprehensive financial services. This includes receivables financing, securitisation, and optimised payables management, all of which provide businesses with greater financial flexibility. By leveraging these capabilities, banks can move beyond simple payment processing and position themselves as strategic partners, helping their corporate clients optimise financial operations while creating new revenue streams.

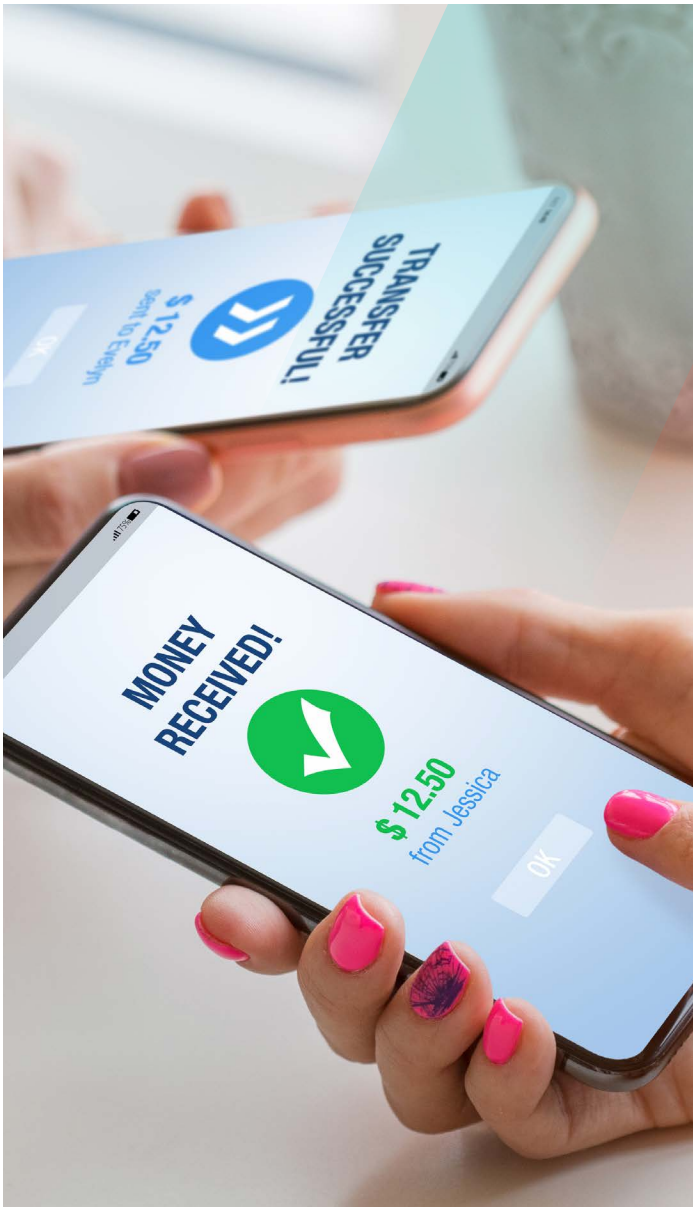
What do you see as the biggest trends in global payments over the next five years, and what strategies should banks adopt to stay competitive and compliant in the evolving global payments landscape?

We're seeing a return to broader discussions about payments growth, and despite economic uncertainty, the outlook remains strong. In the U.S., payments revenue is expected to grow at around 6%, aligning with long-term averages. While this rate fluctuates slightly over time, it remains a solid growth trajectory, especially considering that payments typically account for 35-40% of a bank's total revenue. Over the next five years, this steady expansion is expected to continue, making it a bright spot within financial services.

Interestingly, commercial payments are projected to outpace consumer payments in terms of revenue growth. A key driver behind this trend is the long-overdue digitisation of the accounts receivable and payable value chain. While this transformation has been unfolding for years, it is set to accelerate further. Additionally, small business payments represent a significant profit opportunity. Historically underserved compared to both consumers and large corporates, this segment is now gaining attention from FIs looking to tap into its potential.

On a global scale, real-time payments are entering a phase of exponential growth. Although real-time payments have existed for years, certain markets—including India, the U.K., and Brazil—are now seeing transaction volumes surpassing the trillion-dollar mark. The real catalyst behind this surge isn't just the payment rails themselves but the applications built on top of them. Markets prioritising user-centric payment applications, such as India's UPI and Brazil's Pix, are experiencing the most rapid adoption. Just as a water supply is only useful when connected to appliances like dishwashers and showers, payments infrastructure only reaches its full potential when paired with applications that facilitate P2P transfers, point-of-sale (POS) payments, small business invoicing, and corporate transaction services. In some countries, governments and central banks play a direct role in shaping both the infrastructure and the applications, while in others, market-driven innovation is leading the way.

When it comes to modernisation, rather than large-scale core replacements, banks are taking a more strategic approach with two key models. The first, often referred to as 'hollowing out the core,' involves maintaining the existing core system while modernising everything around it. The second approach, sometimes called a 'sidecar strategy,' introduces modernisation in a controlled manner, often by testing new systems in smaller areas. For example, some institutions start with short-term consumer lending, where loans naturally expire within a year, eliminating the need for system conversions. Others are rolling out updated systems in a digital bank or a foreign subsidiary before scaling the new architecture across the broader organisation. These strategies allow for a more gradual, risk-averse evolution, minimising disruption while still driving progress.



Navigating regulation and compliance in the evolving payments landscape

As real-time payments, open banking, and digital innovation continue to transform the global financial ecosystem, FIs and merchants are under mounting pressure to keep pace with increasingly complex regulatory demands. Regulations such as PSD3 and IPR in Europe and PCI DSS 4.0 are redefining compliance expectations around security, speed, transparency, and data protection—with direct implications for how merchants handle payments, protect customer data, and engage in cross-border commerce.

Key compliance areas

For real-time payments, the focus is on ensuring secure, efficient transactions that align with international standards. Regulators are addressing fraud prevention, dispute resolution, and consumer protection challenges.

Merchants with international customer bases or supply chains must build flexible systems to accommodate local laws while delivering seamless payment experiences across borders.

There is a growing recognition of the need for standardised compliance frameworks to facilitate cross-border payments. Global shifts in payment regulations are pushing countries to adopt uniform standards for real-time payments, consumer protection, and fraud prevention. Institutions and merchants must stay aligned with both domestic and international regulatory changes to maintain global compliance.

Europe: PSD3, PSR, IPR, and VoP

PSD3 in the EU aims to address inefficiencies in open banking, requiring faster, more reliable APIs and improved transparency through performance reporting. PSD3 builds on existing regulations to promote interoperability, consumer protection, and fraud prevention, while also strengthening open banking access and cross-border payment security. Payment Services Regulation (PSR), part of the broader PSD3 directive, replaces PSD2 by converting many payment service rules into a directly applicable EU regulation. This ensures uniform application across member states without national variations. PSR covers operational rules for PSPs, including authentication, open banking API performance, transparency, and risk-based fraud prevention.

The EU's IPR, introduced in 2024 and fully rolled out in 2025, is reshaping how euro payments work across SEPA. It requires payments to be processed in under 10 seconds, 24/7, aiming to boost speed, security, and convenience. The regulation also includes a Verification of Payee (VoP) rule to confirm account details and reduce fraud, like APP scams.

This shift brings faster, more accessible payments across borders, better cash flow for businesses, and no extra fees for instant transfers. It also strengthens fraud prevention and encourages innovation among PSPs, merchants, and fintechs.

For merchants, this means faster settlement of funds, fewer payment delays, and improved customer satisfaction, especially for eCommerce and cross-border transactions.

U.S.: Federal payment modernisation

In the U.S., regulatory momentum is also building. In March 2025, President Trump signed an executive order to modernise how the federal government sends and receives money—eliminating paper checks in favour of electronic payments by the end of September 2025. This shift is designed to boost efficiency, cut costs, and improve security through tools like direct deposit, prepaid cards, and digital wallets.

While exceptions will exist for individuals without access to digital tools, the goal is full participation in a more modern payments system. Federal agencies are now required to create compliance plans, and the U.S. Department of the Treasury will oversee implementation and data protection. This federal initiative complements broader market developments like FedNow, reinforcing the U.S.'s commitment to real-time, digital-first payments.

Accelerating PCI DSS 4.0 compliance—the growing focus on data security

In today's digital-first world, safeguarding sensitive customer information is more critical than ever, especially as businesses face increasingly stringent regulatory frameworks like PCI DSS 4.0. As of April 2025, compliance with PCI DSS 4.0 is mandatory. This updated standard emphasises stronger encryption for cardholder data during transmission and storage, enhanced authentication measures, such as multi-factor authentication, and new client-side security requirements to address vulnerabilities in modern payment systems.

Merchants are among the most directly impacted, as they often store and process payment information across various customer touchpoints, including online checkouts, mobile apps, and physical POS. They must implement real-time monitoring for unauthorised script changes, ensure robust key management, and prove compliance through regular assessments.

Non-compliance can result in steep fines, loss of card processing privileges, and loss of consumer trust following a breach.

Toward standardisation and convergence: The role of ISO 20022

The global shift toward ISO 20022 is a milestone in payments modernisation. This messaging standard offers rich, structured data that supports real-time processing, analytics, and automation. It reduces fragmentation between domestic and cross-border systems and eliminates the need for siloed infrastructure.

However, card payments still rely on ISO 8583—a format not built for extensibility or modern orchestration. As both standards coexist, banks must manage complexity across multiple schemes. A standards-agnostic payments hub is key: it decouples business logic from message formats, enabling banks to apply consistent risk, compliance, and analytics across payment types without costly platform overhauls.

Cross-border payments: Navigating complex compliance requirements

Global commerce is driving a surge in cross-border payments, but with this growth comes a complex set of regulatory challenges. Payment providers and merchants operating internationally must adhere to several local, national, and international regulations, each with their own unique requirements and deadlines. Compliance with global standards is vital to maintaining smooth operations in cross-border transactions. For instance, the EU's AMLD6 requires detailed reporting of high-risk transactions, and payment providers need to update their systems to monitor and report suspicious cross-border activity.

Cross-border payments provide growth opportunities but also increase regulatory complexity. As systems become more connected, FIs and merchants face several challenges in maintaining compliance. For merchants, especially those in eCommerce, navigating varying rules on sanctions, taxes, data residency, and consumer rights adds complexity to scaling globally. Failure to comply can result in blocked payments or legal consequences.

Challenges in compliance

Given the complexity of evolving regulations, FIs and merchants must adopt proactive strategies to stay ahead of compliance risks. Key approaches include:

- **Global standards complexity:** Regulations vary significantly across jurisdictions. PSD3 represents the next phase in the EU's effort to modernise payment services regulation. In North America, U.S. regulators face shifting policies and limited federal authority, complicating compliance—especially around AI oversight—while Canada tightens rules on resilience and cybersecurity. Asia-Pacific sees rapid digital growth—led by India and Singapore in real-time payments—but faces fragmented regulations and cybersecurity challenges. The Middle East and Africa are rapidly embracing fintech, though alignment with global standards and cybersecurity remain key hurdles. In South America, open banking is progressing—particularly in Brazil—but economic instability poses challenges to tech investment and compliance.
- **Technological upgrades:** Real-time payments demand advanced infrastructure capable of processing transactions instantly while maintaining security and compliance. In the U.K., FIs must upgrade their systems to comply with CoP rules. This requires advanced infrastructure that verifies account details before processing transactions, reducing APP fraud risks. Merchants must also ensure their payment gateways, APIs, and fraud detection tools are updated to support real-time, secure processing.
- **Operational risks:** The speed of real-time payments increases the risk of fraud and errors, necessitating robust monitoring systems. For merchants, this means investing in smarter fraud prevention tools and ensuring that customer service teams are equipped to handle fast-paced payment issues.

Strategies for staying ahead

To remain compliant and competitive, FIs and merchants should consider the following approaches:

- **Invest in scalable compliance technology:** Automation tools can streamline monitoring processes and ensure adherence to complex regulations.

- **Adopt agile governance models:** Institutions must build adaptable frameworks that can quickly respond to regulatory changes.

- **Improve collaboration:** Partnering with regulators, industry peers, and technology providers can help shape effective compliance strategies while fostering innovation.

- **Prioritise education and training:** Continuous learning for compliance teams is essential to keep pace with evolving requirements.

How FIs can stay ahead of compliance challenges

As regulatory requirements continue to evolve, staying ahead of compliance requirements will take a proactive approach. FIs and merchants must implement compliance strategies that prioritise agility and adaptability. This includes:

- I**nvesting in regulatory technology (regtech):** Adopting advanced technology solutions can help institutions automate compliance processes, track regulatory changes, and ensure continuous alignment with evolving standards.
- **Regular audits and risk assessments:** Ongoing internal audits and risk assessments are essential for identifying vulnerabilities in existing systems and ensuring that new regulations are met promptly. Merchants should conduct routine reviews of checkout flows, payment data storage, and cross-border payment mechanisms.
- **Employee training and awareness:** Keeping staff informed about changing regulations and compliance protocols is key to ensuring that all departments follow best practices and understand the importance of compliance.
- **Collaboration with compliance experts:** Partnering with regulatory bodies and compliance experts can help organisations stay on top of new developments and navigate the complexities of the regulatory environment.

The role of global collaboration

As financial markets become increasingly interconnected, global collaboration is critical for developing unified standards that address emerging risks. Initiatives like cross-border instant payment systems highlight the need for cooperation between regulators and industry stakeholders to create seamless payment experiences while safeguarding against systemic threats.

Merchants who operate internationally stand to benefit from these harmonised standards, which can simplify compliance, reduce friction, and support growth in new markets.

ACI Worldwide: Powering the world's payments ecosystem

The global payments ecosystem is evolving rapidly, driven by technological innovation, shifting customer expectations, and increasingly complex regulatory landscapes. For banks, merchants, and billers, navigating this dynamic environment effectively is critical.

ACI Worldwide is uniquely positioned at the center of this evolving payments ecosystem. With a presence in nearly 100 countries—and a legacy of 50 years of industry leadership—ACI has been a trusted partner to banks, FIs, PSPs, merchants, and billers around the world, consistently delivering secure, mission-critical payment solutions at scale, supporting billions of transactions and helping customers navigate every phase of digital transformation. For 50 years, ACI has delivered exceptional value and innovation for customers with market-leading solutions that enable secure, scalable, and efficient payment operations worldwide.

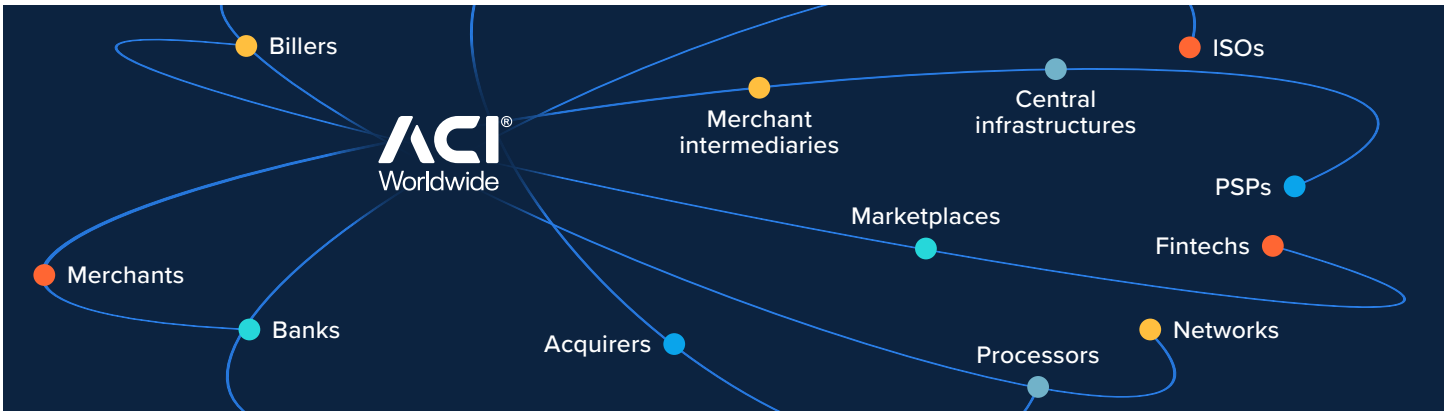
Intelligent payments orchestration: Simplifying complexity and strengthening fraud management

ACI's intelligent payments orchestration provides organisations the tools to manage the complexity of modern payment systems seamlessly. It also strengthens fraud management by using AI-powered analytics and real-time transaction monitoring to reduce false positives, detect anomalies across payment types, and safeguard customers against evolving threats. By consolidating risk signals across channels, ACI delivers a more accurate, proactive approach to fraud prevention that enables higher authorisation rates and greater customer trust. Leveraging cloud-native technology and advanced AI, ACI optimises transaction routing, automates payment workflows, and enhances fraud detection and compliance. This orchestration capability ensures reliable performance with nearly 100% uptime, safeguarding operations and customer data.

ACI Connetic: A modern payments hub built for transformation at scale

Central to ACI's orchestration strategy is ACI Connetic, a transformative, cloud-native payments hub. ACI Connetic consolidates A2A and card payments into a unified, scalable platform, streamlining operations through real-time processing, AI-driven analytics, and robust fraud prevention. With modular design and open APIs, ACI Connetic enables fast and seamless integration into existing systems, allowing banks and FIs to modernise payments infrastructure efficiently and effectively.

ACI Connetic®



Comprehensive solutions for banks, merchants, and billers

Banks: ACI enables banks to consolidate diverse payment systems onto a single, integrated platform. Banks gain comprehensive visibility across payment channels, significantly enhancing operational efficiency and customer engagement. The adoption of standards such as ISO 20022 is simplified, facilitating seamless compliance and interoperability. ACI Connetic's real-time processing and integrated fraud prevention further support banks in delivering secure, trusted payment services. The platform supports dynamic risk assessment and embedded compliance logic tailored to each payment rail, helping banks manage regulatory obligations such as PSD3, AML directives, and instant payment mandates without adding friction to the customer experience.

Merchants: ACI provides merchants with robust solutions that streamline payment acceptance across various channels and geographical regions. Merchants benefit from unified reconciliation and automated fraud management, significantly reducing operational complexity. ACI's orchestration platform enables real-time fraud scoring that minimises false declines while preserving high-speed approvals—helping merchants recover revenue that would otherwise be lost to mistaken rejections or downtime across acquirers. Real-time analytics and intelligent transaction routing capabilities help merchants optimise acceptance rates and reduce payment friction, improving the overall customer experience.

Billers: For billers, ACI transforms billing processes into strategic assets. Its solutions facilitate multichannel bill presentment, real-time payment processing, and automated exception handling. Features like real-time payment posting and intelligent retry logic ensure timely, accurate billing operations. By enhancing digital payment capabilities, billers can achieve improved cash flow management, operational efficiency, and customer satisfaction.

Advancing real-time payments globally

ACI is a global leader in supporting real-time payment infrastructures, currently facilitating 26 real-time payment schemes worldwide. By collaborating closely with central banks, FIs, and payment schemes, ACI ensures tailored, effective implementations suited to local requirements. ACI Connetic further enhances these capabilities with support for cross-border transactions, SWIFT payments, and real-time gross settlement, broadening FIs' reach and efficiency.

A trusted partner for the future

ACI Worldwide remains committed to providing robust, intelligent payment solutions that empower banks, merchants, and billers to thrive amidst a continuously—and rapidly—evolving industry. ACI is dedicated to powering the world's payments ecosystem—delivering secure, scalable, and efficient payment experiences today and into the future.

Literature

ACI Worldwide

- Prime Time for Real-Time Global Payments Report (2024)
- Real-Time Payments: Economic Impact and Financial Inclusion
- 2024 Scamscope Report

BCG & Elevandi

- AI in Financial Services: Making It Happen at Scale

Capgemini

- World Payments Report 2025

Datos Insights

- Vendor Evaluation: Payment Hubs
- Payment Hubs: Why Banks Must Move Forward with Urgency

Deloitte

- 2025 Banking Regulatory Outlook: Gearing Up for Change
- Shaping the Future of Payments: Trends and Insights for 2025

G20

- Cross-Border Payments Project: Staying Ahead of the Curve & Driving Global Change
- Roadmap for Enhancing Cross-border Payments: Consolidated Progress Report for 2024

Juniper Research

- Global Network Tokenization Market: 2025–2029
- Online Payment Fraud: Market Forecasts, Emerging Threats & Segment Analysis 2023–2028

Mastercard

- A Framework for the Interlinking of Instant Payment Systems
- Embracing the Network Tokenization Revolution

McKinsey

- On the Cusp of the Next Payments Era: Future Opportunities for Banks (2023)

MRC (Merchant Risk Council)

- 2025 Global eCommerce Payments and Fraud Report

The Paypers

- The Global Payments and Fintech Trends Report 2025

The Payments Association

- 2025 Payments Outlook: Key Findings from Industry-Wide Survey Data

THE PAYPERS

The Paypers is the Netherlands-based leading independent source of news and intelligence for professionals in the global payment community.

The Paypers provides a wide range of news and analysis products aimed at keeping the eCommerce, fintech, and payment professionals informed about latest developments in the industry.

ACI Worldwide, an original innovator in global payments technology, delivers transformative software solutions that power intelligent payments orchestration in real time so banks, billers, and merchants can drive growth, while continuously modernizing their payment infrastructures, simply and securely. With 50 years of trusted payments expertise, we combine our global footprint with a local presence to offer enhanced payment experiences to stay ahead of constantly changing payment challenges and opportunities.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide, Inc. 2025
ACI, ACI Worldwide, ACI Payments, Inc., ACI Pay, Speedpay, and all ACI product/solution names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries, or both. Other parties' trademarks referenced are the property of their respective owners.

ATL2117 06-25