IDEMIA PUBLIC SECURITY

Identity as Payments & Payments as Identity

We Move Trillions in Value Yearly, But How Do We Know Who It's For?

Amit Sharma

Head of Global and Digital Strategy
& Ecosystem Growth
IDEMIA Public Security

Global payments are constantly evolving, creating new payment rails that expand beyond traditional banking: web-based experiences, real-time peer-to-peer (P2P) and account-to-account (A2A), digitally native wallets, and, increasingly, digital assets enabled via decentralized networks, like stablecoins. This evolution is motivated by faster transaction speeds and "throughput," enabling consumers and institutions to move more value between more counterparties for more reasons, in near real time, across the globe. Doing so requires a number of verifications and affirmations between counterparties, liquidity providers, account/wallet custodians, and other operational and compliance actors and actions to keep the movement of value safe, secure, and protected from illicit actors and fraudsters. In short, sending value *as seamlessly as sending a text or email* requires knowing *who you are sending to,* quickly and with high assurance, in an increasingly murky online environment filled with bots and AI agents.

As digital transactions scale, the old separation between "who you are" and "how you pay" is becoming a bottleneck—creating friction for customers and exposure for businesses. The payments industry remains the most valuable part of financial services, **generating $2.5 trillion in revenue from $2.0 quadrillion in value flows, in 3.6 trillion transactions worldwide.**

At the same time, fraud is becoming increasingly sophisticated, with **much of it rooted in identity compromise,** and amplified by rapidly improving AI. The way forward is to treat identity like a first-class payment instrument: verifiable credentials bound to users through strong, phishing-resistant authenticators, public-key cryptography (PKI), and advanced biometrics. When identity is "tokenized" and cryptographically bound to transactions, moving money can become as easy as proving who you are—and proving who you are can be as simple as initiating a payment. Now is the time to bring high-assurance root-of-trust identity and biometrics into the infrastructure of payments operations itself.

Reshaping Global Payments Infrastructure, Tokenization and Web-nativity

Global payments remain the most valuable layer of financial services. Leading industry trackers project $2.4–$3.0 trillion by 2029, reflecting structural growth even as regional technologies shift and margins compress on real-time rails. Payments are forecasted to reach nearly 40% of global banking revenues by 2027. This represents more than 7% compounded annual growth in certain regions such as Asia—and they are predicted to continue to grow unabated for the foreseeable future. We are rapidly shifting away from the traditional providence of banks and bulge bracket credit card companies to a mosaic of new rails and payment form factors (e.g., payment stablecoins) readily accessible through personal devices and unrestricted by bank operating hours.

Consumers and businesses alike are driving many of these innovations, demanding device- and web-native applications that can provide such connectivity without ever setting foot in, or contacting, a bank or money remitter. Businesses are going cashless across B2B operations, and the tendency of digital assets flows to exploit efficiencies is also reflected in M&A markets, with more processor consolidation (e.g. Fiserv-First Data), merchant services growth, and card networks moving closer to end users while partnering with digital asset networks.

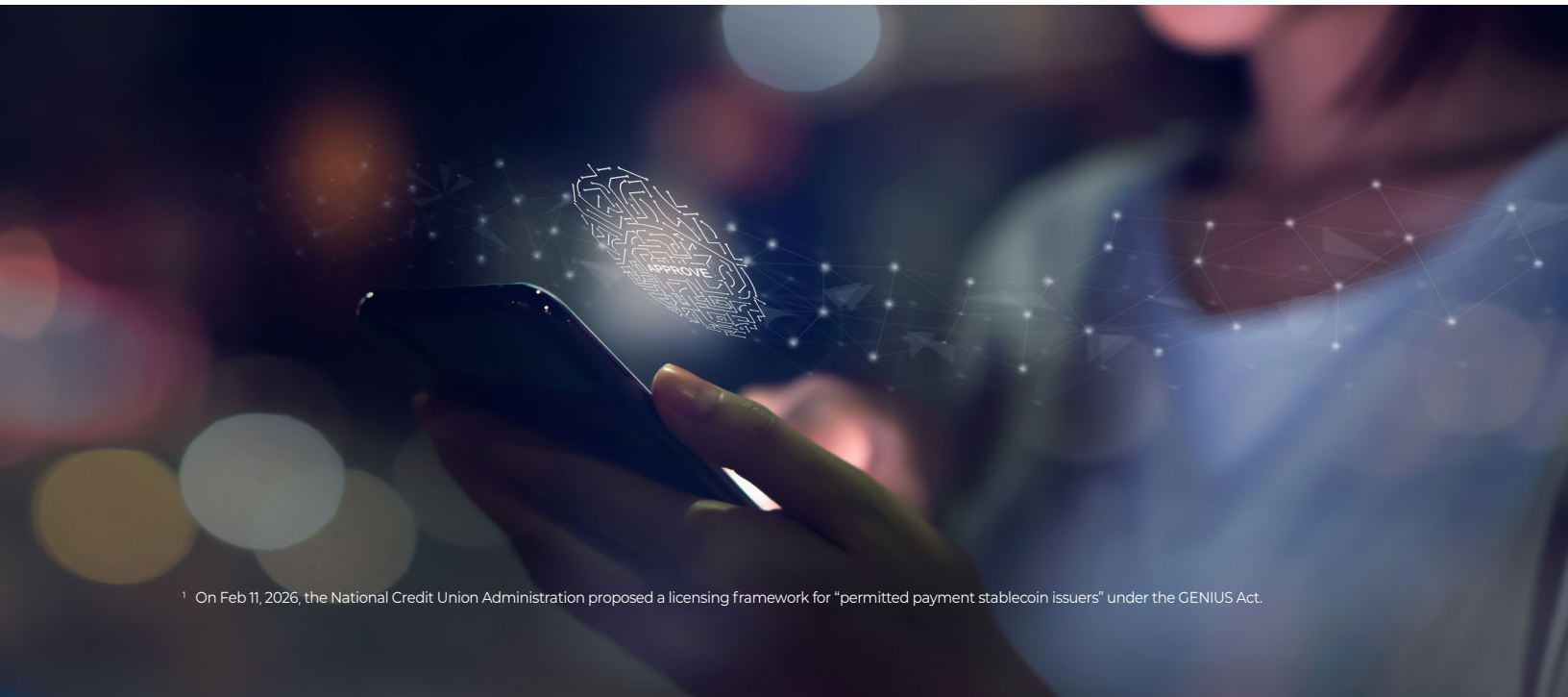
More digital migration means more web-based and mobile experiences; this means more tokenized credentials and wallet/app-based user experiences. Worldpay's GPR highlights wallets' rise across ecommerce and the role of P2P rails, increased merchant adoption, and even unlocked and verified via an individual's biometrics. From retail to institutional, domestic to cross-border, moving value when, where, and what form you need is an increasing possibility.

Some of the most remote emerging markets have seen mobile and cell-phone penetration rates skyrocket, making device-centric applications the explicit growth vector, encouraging merchants, point-of-sale, and in-person transactions as easy as opening an app, tapping your phone, reading a QR code, or even using your face or other biometric. With the ongoing growth in e-commerce, marketplaces, and super-apps, different value ecosystems are continually emerging. Mobile telecom minutes, airline miles, loyalty points, and gaming tokens—are now tradeable between fiat instruments—connectable directly to bank accounts and wallets.

This means the nature of "value" is changing how we transact, and not just on the margins where digital innovation often starts to gain traction, in banking deserts or in areas where financial exclusion remains high; tokenized finance is becoming increasingly mainstream across the largest institutions as well (corporates and banks), enabling supply chains, interbank settlements, foreign exchange management, and even government applications like benefits distribution, reserve management, and central bank digital currencies. Digital money is increasingly entering the fold as more traditional banks (including community banks and credit unions) innovate with stablecoin issuers and crypto exchanges[1]. These efforts signal increasing adoption of digital assets—at the very least fully-reserved stablecoins—and that these assets can sit alongside cards, P2P and wallets, and be integrated between payment facilitators and processors.

In summary, payments innovation continues unabated, filling in the gaps associated with cross-border and segregated rails, and increased digitization of transactions between people and organizations is bringing down barriers that have kept transactions costs high and interoperability challenged.

Notably, a common motivator for ongoing innovation is financial crimes compliance (FCC). Regulators are expanding their focus on payments and transaction banking as geopolitical volatility for market participants grows. As such, anti-money laundering (AML), sanctions compliance, and associated know your customer (KYC) affirmations, and customer information programs (CIP) are increasingly important cross-jurisdictionally, but continue to encounter challenges due to inconsistent policy developments and enforcement mechanisms across countries. Regulators are recognizing that payments flows are increasingly software/data flows across cloud ecosystems; payments now carry "more" data – and it stands to reason that identity applications must follow suit.



[1] On Feb 11, 2026, the National Credit Union Administration proposed a licensing framework for "permitted payment stablecoin issuers" under the GENIUS Act.

The Threat Reality: Fraud Growth, AI Acceleration, and the Identity Nexus

In late 2024, Verizon reported that compromised credentials were a leading initial access vector in breaches (i.e., one-quarter to one-third), with phishing and web app exploitation close behind—an ensuring risk for any payment flow. P2P and A2A growth is expected to grow, in particular as agentic AI is also increasingly adopted. Assistance from AI raises the ceiling and the floor for adversaries: deepfakes, personalized lures, and automated probing scale social engineering. The rapid and ongoing rise of AI applications has literally created "fraud as a service" schemes, and everyone must be vigilant to these threats as online activities grow accordingly. Financial institutions regularly report that AI represents the most transformative technology impacting services and productivity - while also exacerbating threats. Here, too, consumers (individuals and businesses) are acknowledging the need for balance between opportunity and vulnerability. In a recent survey, BCG cited that 80+% of consumers expect to increase their use of agents to undertake payments activities, with younger generations estimating they expect more than 50% of their transactions to be undertaken by agents by 2030. At the same time, a majority of Americans believe AI will make identity theft more prevalent and are themselves demanding greater assurances from their financial services providers that their personal and economic data is protected—and regulatory expectations are reflecting these growing demands.

Policymakers are responding: Treasury's February 18, 2026 initiative delivers practical resources for AI risk management in finance, explicitly integrating fraud and digital identity. Web-nativity and AI convergence means that financial crimes risk is intimately intertwined with anti-fraud tooling, cyber resilience, and operational controls. AI may exacerbate such threats, but AI-enabled tooling is also useful in automating investigations and remediation of potential fraud and exploitation.

Generative AI applications can combine data from KYC processes, client profiles, behavior, and product use to drive real-time screening for suspicious activities, alert-handing, and reporting on fraud, or to work on targeted use cases. With more data traveling alongside payments, so too can affirmative identity data—creating better safeguards for consumer data, while ensuring the transparency of operations needed to protect financial system integrity.

Embedding Identity in Payments Infrastructure

Work is afoot to better equip this fast-evolving payments landscape. We have the tools to turn historically reactive regulatory compliance on payments security to more proactive risk management within analog and digitally native ecosystems. Simple efforts to address online weak points are well underway. Passwords are being replaced by passkeys (FIDO2/WebAuth), where no personally identifiable information (PII) or shared secrets traverse the network. Passkeys are phishing-resistant and origin-bound, and can strengthen multifactor authentication, especially when combined with biometrics.

The growth in use of verifiable credentials (VCs) as digital identities can carry both root-of-trust identity affirmation with other relevant risk-attributes needed for the movement of value (e.g., sanctions status, affiliations, transaction history, etc.). VCs link authentication to authorization where users attest to *their own* attributes (e.g., KYC), and are verified without ever revealing PII.

Growing mDL adoption is a good start; the move to intermediary-issued VCs with user control and permissioning would go further to reinforce identity at the user and device layer and also reduce liability and compliance risk for service providers. Applying advanced biometrics to KYC at onboarding can increase levels of assurance in keeping with the risk-based approach required for financial crimes compliance. Strong biometrics are also the strongest form of protection against agents and AI deepfakes.

By applying VCs at onboarding and throughout the user's lifecycle, benefits are conferred to both regulators and chief risk and compliance officers. Combining PKI with VCs can further bring identity affirmation every time a payment is initiated, and can build in transaction-monitoring controls as every transaction will essentially have a cryptographic tag affirming its legitimacy (or be blocked/revoked if determined to be illicit/unverified) at the time of its execution and not in retrospect, as the majority of anti-fraud and lookback controls are currently executed.

With embedded identity, travel rule compliance (the need to affirm sender and receiver at time or alongside a payment) is automated and secure, regardless if such a payment is made P2P or routed through multiple intermediaries, rails, or payment form factors. Payments services can replace static files with issuer-signed credentials for individual transactions to principals and universal beneficial owners (UBOs) for organizations—strengthening such controls and bringing them into the digital domain. And user affirmations can be limited to a biometric affirmation vs. the continual re-presentment of sensitive PII that can be exploited by illicit actors. Rail-aware orchestration with identity binding means signing payment intents with the same key used for login, creating cryptographic continuity from authentication to settlement, and aligning with tokenized money.

Securing and Simplifying Money Movement by Tokenizing Identity

The payments stack is modernizing: web-native experiences, real-time P2P and A2A, wallets, and supervised, fiat-backed stablecoins and other digital assets. Revenue pools remain massive even as cost pressures and regulation reshape regional efforts, and the barriers for cross-border value movement continue to erode. But the bottleneck—and biggest risk—is **identity.** Stolen credentials are a leading breach vector, and AI is compounding the scale of the threat. The remedy is now practical at scale: privacy-enabled tokenized identity with verifiable credentials; authentication with passkeys and origin-bound PKI; and identity bound to payment intent. Done right, transferring funds becomes as easy as verifying identity—and verifying identity becomes as easy as initiating a payment.

Sources

- **McKinsey** – The 2025 Global Payments Report: https://www.forbes.com/councils/forbesbusinesscouncil/2026/01/12/the-future-of-payments-how-will-money-move-in-2030-and-beyond/
- **Entrust** – Changing Face of Fraud: 2026-identity-fraud-report-re.pdf
- **BCG** – The Future is (Anything But) Stable: 2025-global-payments-report-sep-2025.pdf
- **Worldpay** – Global Payments Report 2025: https://www.worldpay.com/en/global-payments-report
- **PWC** – Navigating the Payments Matrix: https://www.pwc.com/gx/en/financial-services/fs-2025/pwc-future-of-payments.pdf
- **NCUA** – Proposed Rule for Permitted Payment Stablecoin Issuer Applications (GENIUS Act): https://ncua.gov/newsroom/press-release/2026/ncua-proposes-rule-permitted-payment-stablecoin-issuer-applications
- **U.S. Treasury** – Public-Private Initiative on AI Cybersecurity and Risk Management in Financial Services: Treasury Releases Two New Resources to Guide AI Use in the Financial Sector | U.S. Department of the Treasury
- **Verizon** – 2024 Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/dbir.html
- **Fraud as a service** - https://www.thomsonreuters.com/en-us/posts/corporates/faas-new-fraudsters/
- **Passkeys / FIDO Alliance** – passkeys overview and benefits: https://fidoalliance.org/passkeys/

For more information, contact us at **info@ps-idemia.com**

IDEMIA PUBLIC SECURITY

NA.IDEMIA.COM