DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

THE INVISIBLE PAYMENT

It has been 16 years since Uber debuted and ushered in the first embedded-payment experience for many consumers. Today, embedded payments abound and are not confined to a mobile app.

ALSO IN THIS ISSUE:

Volume Twenty-three, Number Three
DigitalTransactions.net
May 2026

Join us at SEAA

June 8 - 10, 2026

Merrick Bank is a proud sponsor of SEAA this year in Miami, FL, June 8-10. Connect with us and see how our clients are at the center of everything we do.

- **Top 15 merchant acquirer in the U.S.**[1]
- **25+ years in the industry**
- **Trusted & reliable partnership**

When you partner with us, you'll have a team of experts available to build a specialized program and help you along the way.

Contact us

[1]by transactions

Merrick Bank

contents

MAY 2026 • VOLUME 23, NUMBER 3

Cover photo: giovanniseabra/123rf.com

Digital Transactions (USPS 024-247) is published online monthly by Boland Hill Media LLC, 800 Roosevelt Road, Building B, Suite 212, Glen Ellyn, IL, 60137.

the gimlet eye

WHY NETWORKS ARE EMBRACING AI

THE TOP BRASS at all the major payments companies is thinking hard about the implications of AI and agentic commerce, the shop-and-spend utility enabled by AI. And for good reason. Most obserers say the technology will spur a boom not only for card networks but for commerce in general.

Indeed, the risk in not deploying AI may well be greater than any risk inherent in adopting it, according to top management at the card networks. Take American Express, just for an example. "You'll see a tremendous creation of new jobs," said AmEx chief executive Stephen Squeri. He brushed aside the looming risk of jobs eliminated by AI while addressing questions last month during a presentation of the company's first-quarter results.

"Technology over time has fueled GDP, not crushed GDP," he argued, referring to gross domestic product, a measure of a nation's overall commercial output.

Under Squeri, AmEx has not been slow to adopt AI and its offshoot, agentic commerce. Yet, much is yet to come from the technology, he promised. "We're warming up in the bullpen on agentic commerce," he said, "We're not even in the first inning."

The company has backed up that sunny forecast in recent months through a willingness to spend on acquisitions. Only last month it announced it has agreed to acquire Hypercard Network Inc., a developer of expense-management technology based on AI, though it did not disclose the terms of the deal.

And, days earlier, it issued a software development kit called Agentic Commerce Experiences, aimed at helping merchants and consumers tackle the new technology.

Risk is a worry, but, ultimately, the way to guard against risk is to have agents "declare [purchase[intent and match [that] with what is actually purchased," said Squeri. "We can get that data. We don't even have that in the physical world." Armed with the right information, AmEx can guard against bad actors, he said. Adding that "If our cardmembers are left holding the bag, we'll back our cardmembers."

Still, despite his optimistic outlook, Squeri conceded agentic commerce "brings added complexity and risk." Facing up to that reality, he said, is the new imperative for payments companies. "We are well-positioned to help protect our cardmembers and merchants," he insisted, promising more AI products will be rolling out later this year.

That AI salient will jostle for resources with other ventures the company is planning for this year, including new or enhanced commercial cards with tools to help manage spending and cash flow. But clearly if AI and its agentic offshoot have the backing of AmEx, you can expect big things from all the networks—and very soon.

John Stewart, Editor | **john@digitaltransactions.net**

MAY 2026 • VOL. 23, NO. 3

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

PUBLISHER Robert A. Jenisch

EDITOR-IN-CHIEF John Stewart

SENIOR EDITOR, DIGITAL
Kevin Woodward

CORRESPONDENTS
Jim Daly, Peter Lucas

ART DIRECTOR/PRODUCTION EDITOR
Elizabeth Novak

Digital Transactions, Digital Transactions News, and DigitalTransactions.net are publications of Boland Hill Media LLC, 800 Roosevelt Road, Suite B212, Glen Ellyn, IL 60137

John Stewart, Managing Director
Robert A. Jenisch, Managing Director

For advertising information, call 630-547-2887. To subscribe or give us a change of address, go to www.digitaltransactions.net and click on "Subscriber Care" or call 630-547-2887.

Subscription prices: $59/year for subscribers in the United States; $69/year for Canadian subscribers. All other subscribers, $119/year, payable in U.S. currency.

BPA WORLDWIDE

The Merchant Supply Partner That Never Misses a Beat

For more than 50 years, General Credit Forms has been the payments industry's trusted partner for high-quality POS supplies.

As the leading single-source provider for merchant supplies, GCF has remained proudly independent – focused solely on serving the needs of our customers. Through every shift in technology and every evolution in payments, we didn't just adapt; we helped shape the path forward.

When reliability matters and experience counts, the industry turns to GCF.

25 YEARS

See us in Miami at SEAA 2026

June 8 - 10

THE COMPANIES OF GENERAL CREDIT FORMS

GCF
GENERAL CREDIT FORMS, INC.

Advanced Labeling Systems · GOLDEN BUSINESS FORMS, INC. · PSI Paper Systems · South Seas Data LLC

www.gcfinc.com · (888) GCF-NEWS

76% OF U.S. COMPANIES SUFFERED FRAUD IN 2025

It's a sobering condition of today's payments industry that fraud is a persistent, pervasive, and unwelcome counterpart to legitimate transaction activity. Testifying to that is that 76% of U.S. organizations experienced attempted or actual fraud in 2025.

That's according to the Association for Financial Professionals' 2026 edition of its Payments Fraud and Control Survey Report.

That 76% figure is down from 2024's 79% and 2023's 80% rates, but the impact is no less troublesome. The data, drawn from 465 responses from treasury professionals and analyzed by Rockville, Md.-based AFP's research department, points away from assuming fraud is episodic, and shows it is much more pervasive.

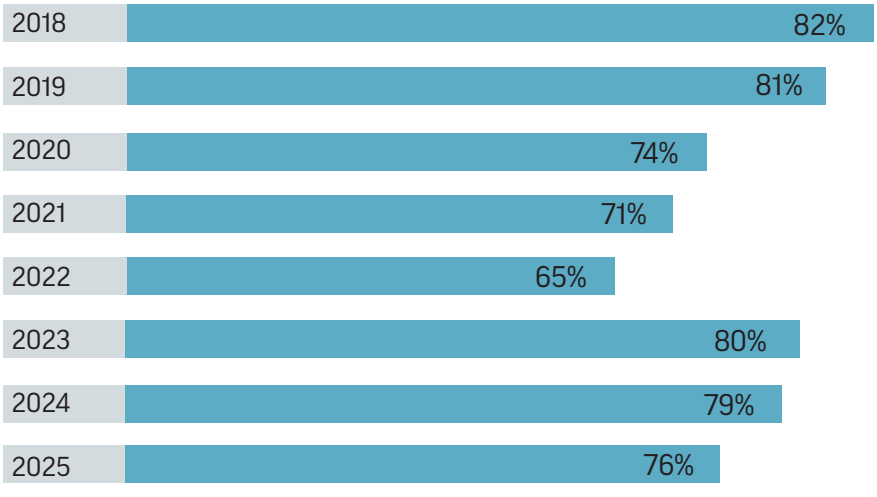
"People used to think of fraud as episodic," says Chris Ward, head of enterprise payments at Truist, a Charlotte, N.C.-based bank and sponsor of the AFP report. Fraud is no longer an exception, "It's more the rule," Ward says.

In practice, that translates to constant vigilance on policies and controls and close attention to fraud activity, he says.

"Payments fraud is increasingly a policy problem, not just a controls problem," Ward says. Organizations, be they banks, payments providers, or merchants, must have the right decisions and the right processes in place to ensure they are protected, he says. That means making the right decisions when a payment is executed, he says.

FRAUD'S STUBBORN PREVALENCE

(Proportion of organizations reporting payments fraud)



Source: Association for Financial Professionals' Payments Fraud and Control Survey Report, 2026 edition

Because payments are diverse and most organizations make and receive multiple types, they need policies and controls for all of them. Conversely, Ward says, criminals only need one entry point to do what they want.

"Remember, the fraudster just has to get one through where, as a company, you've got to protect [your company from] all fraudulent attempts," he says.

While this approach may appear to fit larger organizations well, it also works for smaller ones. Fraudsters do not discriminate and will target any size organization if they sense a payoff.

Some payment types are more prone to fraud than others, and at the top, in the current report, is check and ACH debit fraud. Check fraud was reported by 58% of organizations, the most of any payment type, followed by ACH debit, 30%, and wire transfer, 25%.

They were followed by corporate and commercial cards, 21%, and ACH credits, 18%. New payment types were not immune. Fraud on mobile wallets was reported by 2%, followed by faster payments and cryptocurrency, at 1% each.

Email continues to be the frontrunner in how criminals choose to commit fraud. Business email compromise is the most common threat vector, with 70% of organizations citing it. That's up from the 2025 report, when 63% cited what's known as BEC.

Ward suspects that business email compromise will continue to be problematic, especially as artificial intelligence is refined and criminals adopt it. "It will become harder and harder to detect," Ward says.

This ties into his assertion that managing payments fraud is a quality-control issue. Organizations need to make the right decisions within their payments programs.

Ward suggests organizations not rely on one-time decisions to manage these programs. "Rechecking yourself over and over again, just make sure you're checking your procedures, doing everything you can to protect yourself and taking advantage of every fraud tool and technology available to you," he says.

—Kevin Woodward

TOAST STEERS INTO THE DRIVE-THROUGH LANE

It was only a matter of time before the heated competition for at-table restaurant point-of-sale volume moved to the drive-through lane and attracted front-line payments players. These include long-time providers such as Revel Systems and Oracle. Attracting such players is the potential sales volume. Drive throughs are said to account for between 60% and 70% of sales at outlets that have them.

And now, payments observers can add Toast Inc. to the list of drive-through POS providers.

Known for its at-table POS technology, Boston-based Toast announced last month it is launching Toast Drive-Thru, a unit aimed at winning business from some 140,000 drive-through restaurants estimated to be operating in the U.S. market. The move in part relies on Delphi by Toast, a display system the company acquired in 2023 for an estimated $10 million. Another key feature is AI, which Toast says can cut time and costs by managing orders and displaying them for customer confirmation before payment.

With the technology in hand, Toast says it's ready to replace fragmented drive-through systems and win part of the $140 billion in sales said to be processed through U.S. drive-through lanes. "Brands are constantly being pushed to balance speed and guest convenience with efficiency. At the same time, AI is giving brands new opportunities to impact this equation," notes Steve Fredette, Toast's president and co-founder, in a statement.

But observers caution technology will not by itself be able to account for failed orders or slow lanes for restaurant operators not accustomed to drive-through processing. And big chains like McDonald's have had decades to smooth technical wrinkles, observers say.

"McDonald's, Starbucks, and other players have been supporting drive-through for a long time, and are much better at it, with proven uptime reliability," notes Cliff Gray, proprietor of Gray Consulting, a Chicago-based payments advisory. "Their POS software and [point-of-interaction] hardware is highly tuned to the challenges of drive-through. Toast will have to become very good at POI themselves, proving they can meet the high bar of reliability required, before they can challenge established technologies like these."

On the other hand, operators like Toast may have advantages conferred by experience with restaurant technology. "They are good at transaction data management with their restaurant software," says Gray. "That may prove beneficial to drive-through processing qualification. Likely, drive-through procedures and other differences may teach Toast as much as vice-versa."

The lesson drive-through eateries have learned over the years,

MONTHLY MERCHANT METRIC

Total Gross Processing Revenue %

This is sourced from The Strawhecker Group's merchant datawarehouse of over 4M merchants in the U.S. market. The ability to understand this data is important as SMB merchants and the payments providers that serve them are key drivers of the economy.

All data is for SMB Households defined as households with **less than $5M in annual card volume.**

Metric Definitions: (Only use definitions related to an individual month's release)

Household - Standalone Merchants are considered as a Household with one store and Chained outlets under a common ChainID are combined together and considered as one single Household

Total Gross Processing Revenue % - Sum of total discount, total transaction fee revenue and total other fee revenue divided by total volume

Date	Total Gross Processing Revenue %
Q1'25	2.900%
Q2'25	2.911%
Q3'25	2.942%
Q4'25	2.960%
Feb'26 (T3M)	2.973%

tsg


Gray

> Gray: "In a drive-through lane, if payment acceptance fails, that impacts the whole lane. The merchant could lose [five] sales instead of just one."

Gray adds, is that reliability matters more than anything else. "In a drive-through lane, if payment acceptance fails, that impacts the whole lane. The merchant could lose [five] sales instead of just one," he says.

In the end, reliability and speed will matter more than slick POS, Gray warns. "Toast POS is top-notch, but mission-critical POI is not POS," he says. "Their venture into the drive-thru space will depend on rock-solid POI. Drive-throughs are not countertops or e-commerce."

In the end, much will depend on how much, and how well, Toast learns the drive-through POS market. "They are good at transaction data management with their restaurant software. That may prove beneficial to drive-through processing qualification," Gray says." Likely, drive-through procedures and other differences may teach Toast as much as *vice-versa*."

—John Stewart

PAYPAL'S NEW CEO ISN'T WASTING TIME

Barely three months since taking over the top spot at PayPal Holdings Inc., Enrique Lores is heading up a reorganization of the venerable payments company.

Late in April, PayPal said it will migrate to a three-business operating model. The three are checkout and PayPal, consumer financial services and Venmo, and crypto and payment services.

Lores says the reorganization is part of a plan to "recommit to our fundamentals" and get closer to consumers. Lores was chief executive at computer giant HP Inc. for six years before coming to PayPal.

The Venmo unit will tap into Venmo's momentum, Lores says, and expand into a broader consumer financial-services platform. The PayPal unit will bring the consumer and merchant ecosystems under what he calls a unified strategy, while the crypto and payment-services component will bring operations like Braintree, small-business processing, and cryptocurrency efforts under one roof. PayPal acquired Venmo in 2013 with its Braintree acquisition.

These moves come as PayPal still has strengths it can rely on.

"PayPal still has a stable of strong assets, but many of those assets no longer clearly translate into value for either their merchants or consumers," says James Wester, co-head of payments and research director for technology and infrastructure at Javelin Strategy & Research.

"What's more, the payments market is increasingly competitive, so any value needs to be better than what consumers and merchants can find elsewhere," Wester says in an email to *Digital Transactions News*. "Giving the reorganized units clearer mandates should help with

Continued on page 28

HOW DIGITAL MONEY WILL BECOME NATIONAL CURRENCY

BY GIDEON SAMID
gideon@bitmint.com

CBDC (CENTRAL BANK DIGITAL Currency) is a vision facing mountains of obstacles. It is a long road ahead before this vision becomes reality. Many doubt it. Alas, its future appears guaranteed based on one overlooked factor: taxation.

There are no solid estimates for income-tax fraud, but they approximate around half a trillion U.S. dollars per year. The Internal Revenue Service estimates these figures will explode with the advent of digital currency because the flow of transactions spills out of the banking realm. With this, identities are obscured and money movement becomes undetectable.

Fraud is the domain of the rich, for whom the high investment in the means of fraud pays off. They can hire top talent to outwit government accountants. This dichotomy already creates social pressure demanding brazen progressive taxation, which further motivates the rich to evade payment.

The absence of CBDC invites a host of private coins. Tracking sites report more than 10,000 active cryptocurrencies. They represent a new place to store value and offer a privacy-protected transaction regimen. The government is overwhelmed. As a result, it appears that the old idea of taxing money in motion is reaching its terminal utility. On the other hand, the more basic concept of taxing wealth is becoming that much more attractive.

Whether minted by an automated protocol or by a thoughtful central bank, a digital coin has a public footprint, global visibility. This coin visibility is being paid for by owner obscurity. Ownership is manifest through knowledge of a "private key."

A private key can be stealthily sent from Alice to Bob. That means not only that the key is encrypted but that the very fact that it was sent is undetectable. Bob can then add an extra key to the coin so that Alice cannot send the same key to someone else (double spending). And when this protocol is done, payment has been initiated, consummated and settled in the blink of an eye.

Often times neither payor nor payee wish to expose a transaction, and so the IRS is kept in the dark, shifting the tax burden to the lower classes who still get paid, and pay, the old-fashioned way.

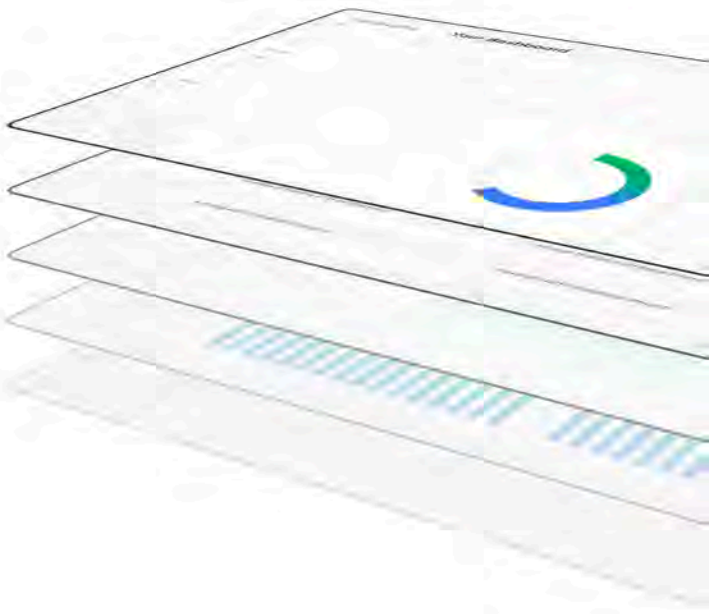
Chasing incomes to fill up the U.S. coffers is becoming increasingly futile. A new concept of taxation is needed, and indeed one invites itself—hinged on public digital coins. Each coin has an owner. This owner presumably benefits from government services. So the government, the mint of the coin, will exchange it with another coin valued (1-x)% of its former value, where x% of the coin is claimed by the government. It is an even burden, not progressive, but fair and fraud-free.

The total elimination of fraud will save the government the currently estimated half-a-trillion-dollar annual loss through direct fraud. Such wealth-based taxation will save the billions of enforcement dollars spent today, while offloading from the public's back the nearly quarter of a trillion dollars spent by all of us, the taxpayers, wrestling with the complicated tax code.

Given that the U.S. dollar is the world's currency, and 50% of U.S. cash is held by foreigners, it turns out that this wealth-based taxation will favor U.S. citizens. That's because so much of the collected taxes will be paid by dollar holders who don't use government services.

The obscurity of digital money keeps many social advocates unaware of the social benefit of shifting the basis of taxation. So this is not an imminent revolution. But when you look beyond 2030, it's hard not to see that wealth-based taxation will become a political hot potato! DT

maverick



Enabling growth for high performing ISOs, ISVs & FIs

Maverick Payments is a privately owned, full-service payments provider that began as an ISO. For over 25 years, we've built a unified platform to help ISOs, ISVs, and FIs manage, monetize, and white label payments across multiple processors and banks. With in house operations, technology, and responsive support, we deliver a reliable engine partners can trust. Our platform enables simpler workflows, faster decisions, fewer surprises, and the scale that supported $25B in annual processing in 2025 for thousands of partners and tens of thousands of merchants.

- Full white label experience
- Digital onboarding
- Streamlined risk & underwriting
- Card & ACH for one dashboard
- Unlimited sub agents included
- Robust portfolio reporting & residuals
- Ticketing & merchant support
- Full stack API

The quickest path to revenue

Grow faster - partner with us today!

800.464.9777
maverickpayments.com

BLUEBIRD'S FAILURE IS STILL A LESSON TODAY

BY BEN JACKSON
bjackson@pa.org

THE END OF A payments era will arrive on June 3, when American Express closes all of its Bluebird prepaid cards. It's the end of a product that seemed to have all the advantages that a payments product could want, but seemingly never made the most of them.

AmEx launched Bluebird with Walmart in 2012, looking for the "unhappily banked," as *Digital Transactions* reported at the time.

The partnership gave AmEx access to Walmart's distribution footprint, and because Bluebird ran on AmEx's three-party network, it wasn't subject to Durbin Amendment interchange caps. It looked like a prepaid product with structural advantages its competitors couldn't match.

Although the prepaid market was crowded and neobanks were starting to appear on the scene, Bluebird stood out: almost no fees, direct deposit, mobile check capture, persontoperson transfers, and access to a feefree ATM network.

Its one drawback at the beginning was that it lacked FDIC insurance, which limited its ability to accept federal direct deposits, but AmEx added it within the first year.

Industry analysts at the time speculated that Bluebird could even become a pathway into AmEx's credit products. The logic was that Bluebird offered deposit and transaction data from consumers who were often thinfile or creditinvisible. If AmEx wanted to expand its customer base, Bluebird could, in theory, have provided information for future chargecard or creditcard customers. But no evidence suggests it ever happened.

Bluebird was created under the leadership of Dan Schulman, then head of AmEx's Enterprise Growth division. That unit was built on the Serve platform and aimed to become an enabler of "digital commerce," Schulman said in early 2012. He described Serve as an enabler of "digital commerce," and he had already struck deals with Sprint and Verizon to preload Serve on mobile phones. Bluebird, in that context, was not a oneoff prepaid card—it was part of a broader plan for AmEx to reach new customer segments and new distribution channels.

So, why didn't Bluebird become a dominant force in American consumer finance? AmEx did not respond to a request for comment, but I have a few ideas.

First, I don't think competition was the biggest constraint. Bluebird had a rich feature set that seems to have anticipated the coming neobank movement. It had subaccounts for families, goalbased savings, mobilefirst money movement, and connections to the Walmart Savings Catcher program. It had the makings of a superapp before that was a thing.

I think the real challenges came from a combination of infrastructure and strategy.

Bluebird and other AmEx prepaid products had a different issuer—American Express Travel Related Services Company Inc.—from the rest of AmEx's products, which are issued by American Express National Bank. Its prepaid products were processed on their own separate platform, the Serve platform.

That likely made it more difficult to integrate Bluebird data into any customer-prospecting programs that AmEx had.

AmEx sold the Serve Platform to InComm in 2017, describing the deal as taking advantage of InComm's prepaid experience. It seems more likely the deal was AmEx looking to spin off a silo that was not part of its central business.

When it comes down to brass tacks, I think Bluebird's relative success reflects that AmEx missed the opportunity that a lot of financial-services companies miss. They can build the customer they want, but they need to organize their products to build customers' financial capacity.

The lesson is to think big picture. How can you take a new product and integrate it into the big picture of a company, its products, its infrastructure, and its markets for long-term strategic goals? DT

celero

A smarter way to scale.

If you're an ISO or ISV, payments are not just a feature. They are a revenue stream, a retention driver, and a competitive edge.

Connect with our team and start the conversation.

Click here

Meet us at at booth 121 at SEAA!

NETWORK TOKENS AND THE NEXT ERA OF DIGITAL COMMERCE

The technology enhances transaction performance while it's fighting fraud and supporting agentic commerce. That will be crucial in the coming decades.

BY **TIFFANY JOHNSON**
Tiffany Johnson is chief product officer at NMI.

Photo: 123RF/vectorfusionart

NETWORK TOKENIZED transactions are expected to double by 2029, reaching an estimated 574 billion globally. That kind of growth doesn't happen in a vacuum. It's being driven by two forces: the pressure to reduce rising fraud and the early-stage shift towards agentic commerce.

If you step back and look at where payments are heading, the signals are consistent and point in the same direction. Merchants want stronger security, lower costs, and better customer experiences. Those priorities aren't new. What's changed is the urgency. Together, they're pushing network tokens from a back-end, behind-the-scenes security upgrade to a core requirement for how digital commerce works.

Network tokens are no longer just about protecting credentials They are becoming the infrastructure that enables more reliable transactions, underpins emerging experiences like biometric checkout, and lays the groundwork for AI-driven commerce.

Indeed, as commerce becomes more automated and competitive, especially for smaller merchants, network tokens are becoming essential to maintaining approval rates, reducing friction, and staying competitive in an increasingly agent-driven landscape. That's why adoption is accelerating across the payments industry, with card networks, payment-service providers, and merchants all pushing to expand their use.

SECURITY FIX, PERFORMANCE ENGINE

Tokenization isn't new. Early approaches replaced card numbers with tokens to reduce risk and limit exposure to sensitive data. That model solved for security. It didn't solve for performance.

Network tokens change the equation. Generated by the card networks and recognized by issuers, they are tied to the merchant and, increasingly, to the device or transaction context. That added layer of intelligence gives issuers greater confidence in each transaction, and that directly translates into higher approval rates and stronger fraud detection.

Network-issued tokens also have the advantage of working across processors, enabling interoperability and breaking down the silos that limited earlier tokenization approaches.

What started as a tool for protecting data is now something more powerful. Network tokens are becoming infrastructure that actively improves how transactions are approved, routed, and completed.

FRAUD: FORCING SMARTER CREDENTIALS

Digital commerce continues to expand, with e-commerce sales in 2025 growing 5.4% year over year. But scale has brought complexity. Fraud is not just increasing, it's evolving, with AI accelerating both the volume and sophistication of attacks. The issue isn't simply more fraud. It's that traditional credentials weren't designed for today's scale and complexity of digital commerce.

Primary account numbers (PAN) and gateway tokens have long played an important role in reducing risk and protecting sensitive data. However, on their own, they provide limited context for issuers, making it harder to confidently assess risk on transactions.

Network tokens build on this foundation. They replace PAN credentials entirely and introduce dynamic, context-rich credentials that issuers can trust. When gateway and network tokens are used together, the result is meaningful. Fraud rates can drop by 28% or more, while legitimate transactions are more likely to be approved. In a landscape shaped by intelligent, AI-enabled fraud, static credentials are becoming a liability.

PAYMENTS: A REVENUE LEVER

For years, payments were treated as a cost center. That mindset, however, is quickly becoming outdated. Payment performance now has a direct impact on revenue. Approval rates, false declines and friction in the checkout flow all influence whether a transaction succeeds or fails.

Network tokens sit at the center of that shift. By improving authorization rates and reducing unnecessary declines, they help recover transactions that would otherwise be lost. At the same time, their lower risk profile can reduce interchange costs, often by as much as 10 basis points.

Those gains add up quickly. For ISOs, PayFacs, and software platforms, this isn't just about efficiency, it's about unlocking incremental revenue and delivering measurable value to merchants.

FIXING SUBSCRIPTIONS

If there's one place where payment failures are most visible, it's subscriptions. Subscriptions have become a key, consistent revenue generator for businesses, enabling recurring revenue without the need to continually resell to customers.

They are also popular among consumers, as they enhance the customer shopping experience and streamline the purchasing process.

Recurring revenue models depend on consistency, but they're often undermined by something simple: card changes. Expired or reissued cards lead to failed payments, service interruptions and, ultimately, customer churn as consumers are unlikely to retry failed transactions or may switch to alternative providers.

Network tokens address this directly. Because they are linked to the underlying account, they update automatically when card details change. There's no need for manual intervention from either the merchant or the customer and no disruption to the customer experience. That continuity matters. In subscription businesses, even small improvements in payment success rates can have an outsized impact on retention and lifetime value.

PREPARING FOR AGENTIC COMMERCE

Today, most transactions are still initiated by people. That's starting to change. Agentic commerce, where AI systems act on behalf of consumers, is moving from concept to reality. Whether it's booking travel, managing subscriptions, or completing routine purchases, transactions will increasingly be initiated without direct input from the user. This shift toward automated commerce raises a new challenge: payments need to carry more context about who or what is initiating the transaction.

With this model for transactions, authentication becomes just as critical as authorization. Technologies like biometrics and passkeys will play a growing role in verifying identity and intent, while network tokens ensure that those interactions can be securely translated into transactions. Together, they create a framework where identity, authorization, and payment are tightly linked for a frictionless payment experience.

Network tokens are well-suited to this environment. They embed trust into the transaction itself, allowing issuers to evaluate activity even when a human isn't actively in the flow. As commerce becomes more automated, payments will become less visible, but the infrastructure behind them will matter more than ever. Network tokens will serve as the foundational layer supporting secure, agentic commerce.

Johnson: Tokens are set for massive adoption.

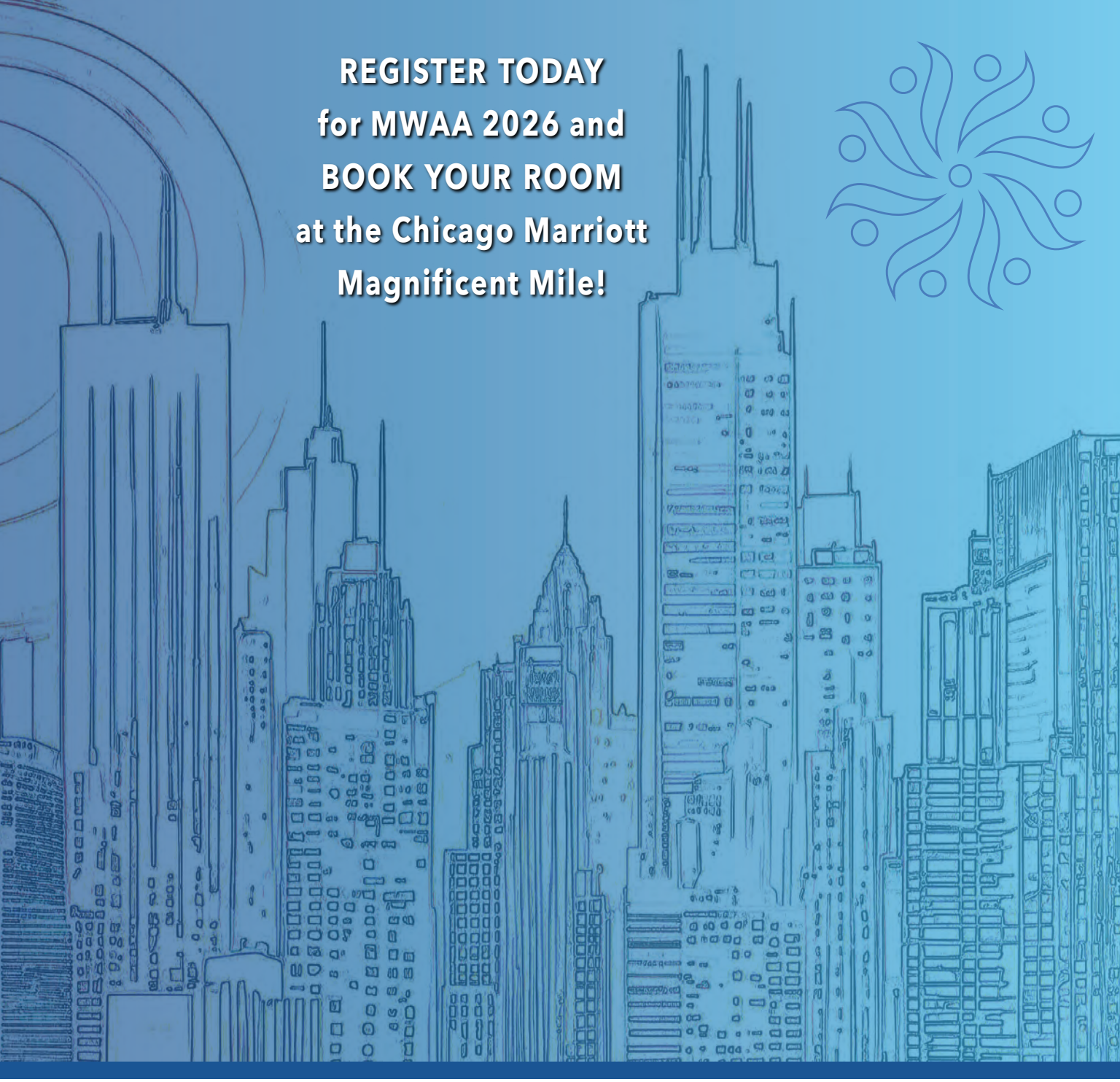
WHAT ALL THIS MEANS

For many merchants, the real cost of payments isn't always visible. It shows up in failed transactions, abandoned checkouts, and lost subscriptions. They all chip away at revenue. Increasingly, it's payment providers that are expected to solve these challenges at scale.

With rising customer expectations for seamless payment experiences, network tokens are quickly becoming a baseline capability for digital commerce, particularly for card-on-file and subscription models. Providers that enable them across their platforms are better positioned to help merchants reduce friction, improve payment performance, and better prepare for the agentic era. At this point, the question is no longer whether to adopt network tokens. It's how quickly they can be implemented across the ecosystem.

The trajectory is clear. Network tokens are moving from optional to essential and will see a massive uptick in adoption. What was once a value-added feature is becoming the default foundation for digital commerce.

As adoption accelerates, network tokens will underpin the majority of card-based transactions, supporting not just security, but the next generation of payment experiences. In the near future, these tokens won't be a differentiator. They'll be table stakes. DT



MWAA 2026

24th ANNUAL CONFERENCE

JULY 22-23, 2026

CHICAGO MARRIOTT MAGNIFICENT MILE

MWAA

MIDWEST ACQUIRERS ASSOCIATION

THE INVISIBLE PAYMENT

It has been 16 years since Uber debuted and ushered in the first embedded-payment experience for many consumers. Today, embedded payments abound and are not constrained to a mobile app.

BY KEVIN WOODWARD

The growth in the availability and use of embedded payments owes much to payment technologies such as tokenization and encryption, not to mention the development of card-on-file applications for consumers and merchants. In practical terms, however, the act of making a payment for a ride share, an e-commerce purchase, a peer-to-peer transfer, or a just-walk-out purchase at an airport shop is just as critical to the role embedded payments play today.

The unseen payment has become the norm for many merchants and consumers. Labeled embedded payments, this method sees merchants making it easy for consumers to load credit or debit card details into an app, for example, to use for all future purchases without having to jump out of the app to complete a transaction. There's no external checkout flow and diversion from the transaction page. It is a native experience, and one that is more and more becoming the norm for many purchases.

Reducing friction in the checkout experience is the goal.

"In general, the consistent and repeatable market force driving embedded payments is the need to remove friction for the user. Indirectly, that need is a result of competitive pressure and consumer demand," says Jeff Wixted, director of product at Signifyd, a San Jose, Calif.-based fraud-prevention company, in an email message.

Amazon.com Inc. was an early pioneer with a 1999 patent on one-click checkout technology. That patent expired in 2017. Then, Uber Technologies Inc. made ride-share payments easier. Other examples are payments for in-flight items, Shopify Inc.'s ShopPay, and the browser version of Apple Inc.'s Apple Pay.

"In each example, the payment is seamless and the focus [is] on the experience, which creates merchant differentiation. I think this is in play across all industries, but certainly most prevalent in retail, travel, and digital (order food or groceries, sports betting, etc.)," Wixted says. "From a risk perspective, the key is to get consistent data elements and signals through the respective sales channel—for instance, mobile, Web, and telephone order—regardless of how the customer wants to pay."

The accelerants driving embedded payments are multiple. It's a tool for increasing consumer stickiness, fixing in-context completion, and driving new monetization opportunities

"Today's consumers aren't focused on payments any more, but rather on the experience," says Jenn Reichenbacher, chief marketing and customer experience officer at Stax Payments, an Orlando, Fla.-based payments company, in an email message.

"Whether it's digital wallets, using social platforms, mobile transactions, etc., consumers are expecting payments to be directly embedded into their experience; it can no longer be a destination," she continues. "As for merchant demand, platforms have to work with what they have, which is why storytelling is so important to drive more revenue and gain more traction. This ties in the competitive pressure. The platforms that are winning are gaining more traction through their effective storytelling, which is gaining customers' trust and value."

She's not alone in this view.

"Three forces are converging," says Dewald Nolte, chief strategy officer at Entersekt, an Atlanta and South Africa-based transaction-authentication provider. "First, behavioral expectations have reset. Consumers and employees increasingly expect instant, in-flow completion rather than being redirected into separate payment steps. Embedded payments meet

that expectation by collapsing steps and reducing abandonment.

"Second, merchant and platform economics are pushing payments upstream. Many software platforms now view payments not as a utility, but as a monetizable layer that improves retention and adds recurring, usage-based revenue. This creates a strong incentive for catch-up adoption by platforms that are still underutilizing their monetization of payments," Nolte says.

"Third, there's competitive pressure from platforms: vertical SaaS and marketplaces are bundling payments into operational workflows (booking, invoicing, claims, procurement), which changes customer expectations across entire industries, not just within fintech." SaaS refers to software-as-a-service.

'Seamless And Trustworthy'

Independent sales organizations and payment processors are keenly aware of the value of acquisitions or of forming partnerships to expand their embedded-payments capabilities. In 2024, NMI LLC launched NMI Payments, a modular embedded-payments service. Worldpay, now owned by Global Payments Inc., launched its Worldpay for Platforms service in Canada and the United Kingdom in 2025, the same year that e-commerce platform BigCommerce adopted technology from PayPal Holdings Inc. for an embedded-payment service.

Embedded-payments capability does more than make in-store and online transactions more seamless. It also has a role in more expedient situations, such as paying for transit.

"For providers, they offer streamlined sales and payment processes that facilitate conversion and, depending on the industry, can represent a competitive advantage or, at least, not falling behind competitors," says Paulo Ferreira dos Santos, chief executive of UbiRider, a Portugal-based transit platform company. "For consumers, they represent seamless and trustworthy purchase processes."

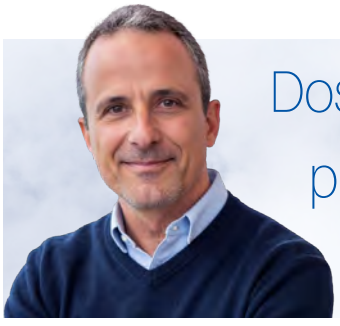
That seamless expectation is overflowing into business-to-business payments, too, says Murray Sharp, senior vice president and global head of B2B at Montreal-based Nuvei Corp.

"Embedded payments in B2B are being pulled by demand, not pushed by providers," Sharp says. "Businesses are digitizing workflows that were historically manual, particularly checks and invoice-based payments, and payments have to follow. At the same time, user expectations have shifted. Finance teams now expect the same embedded, seamless experiences they encounter in consumer apps. That gap is forcing B2B software platforms to evolve."

That ease of use and sense of trust can add to the perceived value consumers can attach to merchants that make an embedded payment possible. That may improve the odds a consumer will return to the merchant's site. A Boston Consulting Group report found that attrition rates for software platforms with an embedded-payment option experienced attrition rates up to 2.5 times lower than platforms without that option.

Other merchant segments see the benefits of embedded payments. Nolte points to marketplaces and travel as industries where payments are not a separate activity but the final step of a workflow. Reichenbacher says industries as diverse as retail, health care, travel, and B2B software-as-a-service have embraced the payment method.

"All of these industries are fully integrated with payments because it's no longer adjacent, it's embedded," she says. "Having these payments embedded into platforms across different industries drives home the idea that payments are central to product experience. These industries want payments in systems they already use, making it easier and faster for them."



Dos Santos: "For providers, [embedded payments] offer streamlined sales and payment processes that facilitate conversion."

Cygma®

BUILD WITH A DIRECT PROCESSOR!

Maximize your revenue potential and take control with Cygma®, Electronic Payments' wholly-owned frontend authorization and backend clearing platform.

- **Same- & Next-Day Funding**
- **Later Funding Cutoff Times**
- **ISV Integrations**
- **Lower Rates & Interchange Optimization**
- **Support for More Terminals, POS & Gateways**
- **Fast Residuals—Paid on the 5th Every Month**
- **Massive Bonuses—Up to $100K!**
- **Access more verticals: CBD, smoke & vape, adult retail & entertainment, MOTO firearms, and more!**

WHY BUILD ANYWHERE ELSE?

Cut out the middlemen and expand with a true end-to-end payments and POS partner, 100% in-house and built to help YOU scale.

RESIDUALS.COM
keith@electronicpayments.com
631-591-7679

Powered By ElectronicPayments®

Adoption and Trust

It's the payment aspect that drives interest and adoption for embedded payments. An easier-to-make payment usually means more payments. More payments mean more revenue. More revenue means funds to grow and develop new products and services.

None of this, of course, comes without risk. Wixted says any embedded payment-enabled platform needs to have consistent data elements and signals in the respective sale channel, whether that's mobile, Web, or a telephone order, regardless of how the customer wants to pay. "At times, a rush to meet consumer demand can cause data to be missing or inconsistent and fraud can quickly result because of a lack of visibility," he says.

Nolte's comments align with that. "From a security perspective, the biggest shift is that embedding payments expands the surface area for scams and social engineering, so adoption and trust rise together only when providers bake in strong authentication and shared risk signals across channels," he says.

Each organization that touches an embedded-payments flow need to assess and understand the associated risks. That's what Peter Uselman, director of partner experience at Madison, Wis.-based Wind River Payments, urges.

"The biggest risk right now is platforms taking on more than they're operationally prepared to manage," Uselman says. "As software providers move toward more embedded or white-label models, they're increasing their exposure to chargebacks, fraud, underwriting, and PCI scope, often faster than expected. Many teams don't account for how quickly that compounds as payments volume grows."

Managing risk means having an intentional design, he says. "The strongest platforms are deliberate about how risk is split with their payments partner. They build protections into the product, keep PCI scope as narrow as possible, and rely on partners for underwriting, compliance and risk. That's what allows payments to scale without creating new problems for the platform or its customers." PCI refers to the Payment Card Industry data-security standard.

Risky Business

Along with a coherent embedded payments strategy, technical and risk aspects must be faced.

Integral to embedded payments is application programming interface coding, which enables disparate software applications to exchange data with each other. It is a foundational element.

Another technical factor is the permission model, Nolte says.

"Consent, authentication, and secure access are increasingly expressed through common patterns (for example, PSD2-style account access and payment initiation concepts), which makes it more practical to embed account-based payment experiences into non-bank journeys," he says. "APIs made embedded payments possible, but standardized consent and authentication models make them scalable." PSD2, or Payment Service Directive 2, is a European regulation governing online security.

Others agree. "APIs made embedded payment possible at scale," Uselman says. "They lowered the barrier to integrating payments into software and made it easier to move quickly."

That said, the technical aspect is not much of a challenge any more, Uselman says. "Most platforms can embed payments at this point. Where things tend to break down is everything around it. Teams add new capabilities or replatform, but don't address onboarding, activation, or how the product is actually used day to day," he says. "We see a lot of teams add new payment capabilities or replatform without fixing the fundamentals underneath. Integration alone doesn't drive usage."

Reichenbacher: "Consumers are expecting payments to be directly embedded into their experience; it can no longer be a destination."

Soares: "Embedded payments in health care come with risk. At each interaction point, data security and HIPAA compliance needs to be upheld."

In a complex environment like health care, APIs can make integrations between software and payments platform less work.

"API-driven infrastructure removes the need to have separate systems and allows embedding payment functions directly in practice management, communication tools, billing workflows etc.," says Thiago Soares, chief operating officer at iCore, a Coral Gables, Fla.-based software developer specializing in dentistry. "It maximizes operational efficiency, with clever algorithms processing requests during patient care and billing of the clinical event itself."

Risk, too, has a role, especially in a health-care field that has specialized privacy regulations.

"That said, embedded payments in health care come with risk. At each interaction point, data security and HIPAA compliance needs to be upheld. Enterprises must thus develop a robust governance framework that layers compliance risks over conversion opportunities," Soares says.

The Role of AI

Risk also carries an undercurrent of uncertainty. In today's commercial and consumer transactional area artificial intelligence is at the top of that trend.

Artificial-intelligence applications in payments, not just the embedded variety, remain a work in progress, says Wixted.

"I think OpenAI discovered how difficult the payment and integration pieces can be when they walked back their 'Instant Checkout' feature, which was designed to allow users to make purchases directly in the ChatGPT interface," Wixted says.

"Instead," he continues, "they are now pivoting to have the checkout occur on the merchant's platform and [are] focusing their energy on search and discovery. In some respects, it is a wise move as it allows consumers to take advantage of their embedded payments and loyalty with the merchant, something they are already familiar with today." OpenAI, backer of the ChatGPT AI engine, had sought to handle payments inside the engine, but revised that approach earlier this year.

With AI and AI agents only in the nascent stages, there appears to be time for AI utility to be worked into embedded payments.

When, or if, it comes, Nolte suggests intent will take on a larger role. "AI pushes embedded payments from 'in-flow checkout' to intent-driven commerce, where the payment moment is triggered by predicted need, conversational decisioning, or delegated action," he says. "AI doesn't just embed payments deeper; it changes who is clicking. The trust model has to evolve from transaction approvals to mandate-based authorization."

Since the debut of the first modern API, generally cataloged as a Salesforce API released in 2000, the technology, and the payments and regulatory infrastructure that makes it possible, have ballooned in uses.

Market and competition pressures may make embedded payments even more appealing, given the simple experience it provides consumers, though the development work may not be so easy for every organization.

And the push to adopt embedded payments may only be increasing.

"At the same time, businesses are dealing with higher costs, more fraud, and more complexity," Uselman says. "They're pushing platforms to simplify payments and help them manage those challenges. That demand is pushing platforms to embed payments more deeply into the experience." DT

HOW GENERATIVE AI IS REWRITING EXPENSE FRAUD

AI-based fraud can cost corporations millions in payments for fake expense reports. Is there a way to stop the theft?

BY **AMIRTHARAJ KARUPPAIAH**
Amirtharaj Karuppaiah is chief technology officer at Oversight.

Photo: 123RF/pressmaster

AT THE END OF every month, finance teams process payments for thousands of expense reports, reviewing airfare receipts, client dinners, conference travel, office purchases. Most look perfectly normal.

Hidden among them, however, may be something entirely synthetic—a receipt that never existed, generated by AI in seconds and designed to look indistinguishable from a real transaction. This is the new frontier of expense fraud.

Generative AI can now produce highly realistic financial documents at scale. These receipts replicate vendor logos, formatting patterns, pricing structures, and timestamps with alarming accuracy. What once required skill and time can now be created instantly with a simple prompt.

Modern generative models are trained on vast datasets of documents, invoices, and transactional artifacts. When prompted, they do not simply "draw" a receipt. They synthesize statistically consistent financial artifacts, replicating layout structures, vendor-naming conventions, tax formatting, currency patterns, and itemization styles.

In other words, these receipts are not crude forgeries. They are synthetic financial documents built from learned patterns of legitimate transactions and used to extract payments from unwary companies.

The result is a fundamental shift in financial risk. Fraud is no longer limited by human effort. It is now algorithmically scalable.

THE RISE OF AI RECEIPTS

Just a few years ago, fraudulent receipts were relatively easy to spot for companies with proper controls in place. A blurry font or

JOIN US IN MIAMI BEACH • JUNE 8 - 10

25 YEARS

SEAA 2026 • MIAMI

THE LATEST TRENDS, NEWEST TECHNOLOGY, AND LEADERS FROM THE PAYMENTS INDUSTRY

Register now for a truly rewarding event that brings payments industry leaders together to help equip agents and sales offices with the knowledge and tools to be more successful. SEAA 2026 is the perfect time for you to network with payments industry leaders, get a first-hand look at the newest technology and grow your business with the latest product offerings. But spaces for exhibitors are filling fast – visit us online to reserve your spot now!

FOR REGISTRATION, AGENDA AND UPDATES

WWW.SOUTHEASTACQUIRERS.COM

a suspicious vendor name was a minor imperfection that indicated potential fraud. More important, fraud was constrained by human effort. It took time and skill to fabricate realistic documents, making most small-scale receipts not worth the effort. AI has removed those limits.

Today, financial documents that mirror real vendors can be produced in seconds and multiplied across thousands of submissions. To generate a fraudulent receipt, all someone needs to do is prompt an AI engine with a request such as: "Generate a realistic receipt from Restaurant X in Atlanta, dated February 24, for a total of $522." The model will then analyze thousands of real receipts from the requested restaurant and generate a single receipt that matches the prompt's specifications exactly.

Some large-language models, including ChatGPT, incorporate safeguards designed to prevent the generation of fraudulent receipts, such as refusal policies that block such requests. Additional barriers exist beyond the model itself. AI cannot generate valid transaction IDs or reproduce the embedded metadata present in authentic receipts. However, these protections are not absolute and can be easily missed during manual review.

Security researchers increasingly refer to this emerging category as synthetic fraud, financial artifacts generated by algorithms rather than manipulated by humans. In the expense-management domain, this means AI-generated receipts, invoices, or travel documents that appear authentic but have no underlying transaction.

Unlike traditional fraud, synthetic fraud is programmable, scalable, and increasingly difficult for human reviewers to detect.

THE FAULTS WITH LEGACY CONTROLS

Finance controls have historically been built around human review and judgment, involving manager approvals, finance-team reviews, and periodic audits. These systems rely on human oversight to identify and flag anything that looks out of the ordinary.

Traditional expense controls were designed for a different era, an era when fraud required effort, time, and human skill. Manager approvals, random sampling audits, and manual receipt reviews were effective when fraudulent documents were rare and often poorly fabricated.

Traditional manual audits review only a small, random subset of receipts and usually occur only after reimbursements have already been issued. When auditing, human reviewers focus on obvious red flags, such as unusually high spend, duplicate submissions, or suspicious timestamps.

But these controls were never designed to defend against machine-generated fraud operating at scale. That is no longer today's environment.

AI-driven fraud now stays within normal ranges, quietly bypassing legacy checkpoints. Without the ability to analyze patterns across thousands of submissions or access embedded metadata, manual oversight is increasingly ineffective.

In an AI-driven fraud environment, manual review becomes mathematically insufficient. When fraud can scale across thousands of transactions, even a small percentage of undetected activity can translate into significant financial losses.

THE IMPACT ON PROFIT

While one or two fake receipts may seem insignificant, AI enables this type of fraud at a scale never before possible, making larger organizations particularly vulnerable. Consider a finance team that processes 5,000 expense reports per month, with an average reimbursement of $200. That represents $1 million in monthly expense volume.

If just 2% of those expenses are fraudulent and go undetected, the


Karuppaiah

Karuppaiah: It's crucial to tell whether the action a user wants to make aligns with his or her intent or that of a criminal manipulator.

result is $20,000 in losses each month, or $240,000 in a year. If the fraud rate rises to 4%, losses climb to $40,000 per month and nearly $500,000 per year.

This simple calculation illustrates how even a small percentage of undetected fraud can translate into substantial financial impact, especially as AI-generated receipts increase in volume and sophistication. Across large enterprises processing tens of thousands of monthly expense transactions, even small fraud rates can quietly compound into millions of dollars in leakage over time.

As if this weren't bad enough, the consequences extend beyond the immediate financial loss. When fraudulent documents enter financial records, audit costs rise as auditors spend more billable time verifying expenses. Budget accuracy can also suffer, as finance teams make planning decisions based on data that has been quietly distorted by fraud.

FINANCE RISK INTELLIGENCE

To address this new arena for fraud, a new operational category has emerged to help enterprises evolve: Finance Risk Intelligence (FRI).

According to the Everest Group, a global research firm, FRI offers a layered, AI-powered approach to risk management. It processes and analyzes thousands of transactions in real time, integrating seamlessly with systems such as ERP, accounts payable, expense management, procurement, and payments.

Everest Group's research shows that while finance operations have modernized rapidly, risk management has struggled to keep pace. FRI helps close that gap by enabling organizations to move beyond traditional, retrospective controls.

Rather than relying on periodic audits or manual review, FRI platforms continuously analyze financial activity across enterprise systems, including expense management, procurement, accounts payable, and payments, identifying patterns of risk as they occur. In other words, FRI represents a transition from reactive financial controls to continuous, AI-driven risk intelligence.

For AI-generated documents, FRI systems look beyond surface appearance and analyze deeper signals, such as metadata consistency, formatting structures, submission timing, and relationships between fields. These indicators are often invisible to the human eye, but FRI can analyze thousands simultaneously and compare them against continuously expanding datasets.

Generative AI has permanently changed the economics of financial fraud. What was once difficult and rare can now be automated, scaled, and hidden in plain sight. But the same technologies that enable synthetic fraud also enable its detection.

In the coming years, the most resilient finance organizations will be those that embrace this reality: in an AI-driven world, the only effective defense against AI-powered fraud is AI itself. DT

WHY PAYMENT LEAKAGE IS A PROBLEM—AND HOW TO STOP IT

Here's why lost revenue from broken payments, once seen as a cost of doing business, are now a strategic priority.

BY CHARLES ROSENBLATT
Charles Rosenblatt is chief executive at Butter Payments

MANY CHIEF FINANCIAL officers assume failed payments are an unavoidable cost of doing business. In reality, a significant portion of that lost revenue comes from customers who want to stay and are pushed out by preventable friction.

CFOs, it's your responsibility to ensure payment systems are accurate, operationally aligned, and ready for long-term growth and success. That's why it's crucial to see payment leakage for what it is: a strategic priority—not a simple backend, technical issue.

When neglected, payment leakage quietly erodes retention, distorts performance metrics, and limits long-term growth. Discover what you can bring to the table by tackling payment leakage with a collaborative, big-picture approach.

Though payment leakage has only emerged as a critical, top-of-mind issue relatively recently, it's always been a silent threat for subscription and usage-based businesses; they were just unaware of it. Payment leakage was simply undetectable until technology caught up. With the right machine learning and large data sets in place, businesses can now uncover previously hidden revenue lost to failed payments, data gaps, and involuntary churn.

According to Boston Consulting Group, 45% of surveyed leaders describe payment leakage as an occasional problem for their business or as an ever-present issue. Yet awareness alone doesn't change the outcome. CFOs need to understand payment leakage to minimize it as much as possible, optimize customer-retention spending, and gain an outsized advantage over companies that still treat leakage as a technical issue.

SAFEGUARDS

Offering convenient payment options is essential for any business, but there must be due diligence before a payment type is rolled out. For example, if you accept prepaid cards for your subscriptions without any caveats, it's only a matter of time before payment leakage will set in.

In fact, we recommend that subscription brands avoid prepaid cards altogether, as by design they inevitably fail, leading to

subscriber churn. However, if a large segment of your customers prefers or relies on prepaid cards, you must implement safeguards to improve forecasting, attract and retain customers, and increase your revenue.

Industry benchmarks show that approximately 15% of payment transactions fail. That failure doesn't always mean lost intent. This is where predictive analytics becomes essential. Instead of waiting for payments to decline, businesses can use historical transaction data and customer behavior to identify subscriptions at high risk of failure—then intervene early with card update prompts, alternative payment options, or tailored outreach.

Predicting problems before they happen shifts recovery from a reactive process to a proactive growth strategy.

Businesses should design experiences around customer preferences and recovery success. The user experience (UX) should include clear, actionable error messages and thoughtfully timed follow-up communication across channels, such as SMS, voice, or email.

The more a company understands the root causes of payment leakage—expired cards, insufficient funds, outdated information, or higher failure rates on certain payment types—the better it can reduce the risk of churn. Tracking key metrics, such as total churn rate, failed payment rate, recovery rate, time to recovery, and revenue recovery, provides a clear operational view of retention performance.

BEYOND FAILED PAYMENTS

Taking a siloed approach can also leave your business in a vulnerable position. Payment leakage is rarely owned by a single team, and that's part of the problem. It's essential for Finance, Product, Marketing, and Customer Operations to know when customers leave and to understand the reasons for their exits.

Here are some common questions you'll face: *Did the customer love the product, but their payments suddenly stopped working? Did they achieve all they sought from using the product? Was the marketing or positioning misaligned—leading them to realize it wasn't a great fit after signing up and taking it for a spin? Is the product faulty, confusing, or missing a key need?*

Thankfully, as CFO, you're in a unique position to bring all of these teams together. Once you have shared visibility across multiple teams and full oversight, you can make sure the right department is aware of the problem.

CFOs are trained to focus on costs, but costs alone don't tell the whole story. For example, let's say it costs you 3% to accept credit cards and 1.5% to accept debit cards. But then you look at your data and see credit card payments have been successful 100% of the time and debit cards have been successful 80% of the time. That "savings" on fees may be quietly costing you 20% of your profit margin.

Costs don't reveal whether different payment methods lead to different behaviors and different lifetime value (LTV). Most companies and CFOs aren't looking at LTV by payment type—and that's a missed opportunity. When you use a product that helps you predict and detect payment leakage, you can increase your LTV per payment type by 5% to 10%, resulting in a material ARR lift.

This transforms the issue of payment leakage from preventing revenue loss to increasing top-line revenue. It's worlds away from simply predicting costs.

With deeper insights and visibility across teams, CFOs can turn lost revenue into a strategic advantage. Smaller firms gain cash flow and stability, while larger firms strengthen retention and LTV. Payment leakage is no longer just an operational concern. It's a financial priority hiding in plain sight. DT

Trends & Tactics continued from page 7

that, but the new structure will need to lead to better product decisions. A focus on trust, simplicity, and good products were what made PayPal so important to begin with. Any reorganization should be judged by whether it helps PayPal get back to that mindset."

The reorganization also is an admission of what the market has known for years, says Stewart Watterson, strategic advisor at Datos Insights: running checkout, Venmo, and payments infrastructure under one undifferentiated roof was limiting all three.

The new structure gives each business a clear identity and someone accountable for it. "Venmo finally gets a real shot at becoming a consumer financial-services platform," Watterson says. "The crypto unit gets a credible infrastructure frame rather than a marketing badge."

In its Feb. 3 fourth-quarter earnings call, led by then interim chief executive Jamie S. Miller, PayPal cited Venmo as a product that was doing well. Not including interest income, Venmo's 2025 revenue reached $1.7 billion, a 20% increase from 2024, Miller said.

PayPal also noted its enterprise-payments business had seven consecutive quarters of profitable growth and its buy now, pay later product generated more than $40 billion in total payment volume last year, another 20% increase.

PayPal's online branded-checkout efforts, which launched in 2023 under then CEO Alex Chriss, were too optimistic, Miller said.

"We've reimagined a product that had been stagnant and underinvested in for years, creating a new value proposition for merchants and consumers," she noted then, according to a transcript provided by PayPal. "But we were too optimistic about how quickly we could drive change and customer adoption across a massive global user base. The results are not yet where we expected them or want them to be."

PayPal also made several personnel moves in April. Heading checkout solutions and PayPal is Frank Keller, who had been general manager of its large enterprise and merchant-platform group. Alexis Sowa, listed as senior vice president and general manager of Venmo on her LinkedIn profile, will lead the Venmo and consumer financial services line on an interim basis. Jeff Pomeroy will be the interim head of the payment services and crypto business.

PayPal also appointed Anshu Bhardwaj, whose LinkedIn profile listed her as senior vice president of PayPal engineering, to the chief AI transformation and simplification officer role. Antonio Lucio, whose LinkedIn profile listed a previous position of executive vice president, chief of marketing, and corporate affairs officer at HP Inc., joins PayPal as chief marketing and corporate affairs officer.

—Kevin Woodward


Lores

PayPal's Lores: A three-business operating model for a struggling PayPal.

Co-Branded E-Mail Marketing

Get the Results You Need

Here's how it works

You select the part of *Digital Transactions*' subscribers you want to reach, sorted how you need it, by function, location, or title. Just ISOs? No problem. Just executives on the East Coast? No sweat. Just CEOs? No worries. Or choose our entire circulation base. It's up to you! You give us your HTML creative. We create both a text version and a Web version of the e-mail deployment. After the deployment, we track deliveries, opens and clicks, and give you all the stats.

It's really that easy!

To get started, contact Bob Jenisch today.

630-547-2887

bob@digitaltransactions.com

Digital Transactions News

We deliver the **payments industry news** to your email inbox daily!

- We have been delivering the payments industry news to your email inbox every day for 20 years
- Digital Transactions News is packed with news and information from the 164.3 billion transactions industry
- Two original stories every issue
- Trending stories, so you know what the industry is reading
- Links to Digital Transactions monthly magazine
- Calendar of events
- Plus "In other News" The most complete listing of announcements from the payment community

Subscribe today at **bolandhill.omeda.com/dtr/**
or email **Bob Jenisch** at **Bob@digitaltransactions.net**