

DIGITAL[®] TRANSACTIONS

Trends in the Electronic Exchange of Value



Say Goodbye to the Passive Wallet

Digital wallets are morphing from credential vaults into active payment orchestrators.

ALSO IN THIS ISSUE:

The Real Value of Payments

Stablecoins vs. Tokenized Deposits

Fighting Fare Evasion, Part I

Payments Under Pressure

Volume Twenty-three, Number Seven
DigitalTransactions.net
October 2026

Co-Branded E-Mail Marketing

Get the Results You Need



**AMERICAN EXPRESS
NO LONGER SETS
THE RATE.**

With Optima, the rate is up to you or your processor. And this kind of flexibility can help you close the deal with Merchants and offer even better service.

See the rate that works for you and your Merchant.

Learn More

"We go back to our service provider annually, and we ask for our rates to be reviewed based on our volume. We just find that your American Express rate for our business."

— Brian's Candy, Great Merchants USA



**ingenico
GROUP**

Your Complete Guide to Payment Security / PCI, P2PE, and more

RECORDED WEBINAR
Watch this recorded webinar PCI at the POS / What's New, What's Next, and What Merchants Can Do to Stay in Compliance to really gain a clear understanding of the Payments Compliance Industry Data Security Standard and its latest updates. Our payment security experts answer frequently asked questions such as:

Watch Webinar & View SlideShare →



**TOP 3 WAYS
to Grow Your Opportunities with**

BlueStar

Download the PDF Starter Kit and avoid leaving money on the counter.

Today's mobile solutions with integrated peripherals make it easier than ever to add revenue within your existing client base. Let BlueStar show you how.

GET THE KIT

What's included:

1. The Top 3 Business Growth Opportunities
2. Steps to Obtain a Dealer License
3. Areas to Expand in the Marketplace



elevate | FUNDING

No credit checks.
No application fees.
Ever.

Direct access to underwriters.
Syndication opportunities.
ACH or credit card splits.

www.elevatefunding.biz

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

contents

OCTOBER 2026 • VOLUME 23, NUMBER 7

Say Goodbye to the Passive Wallet

16

Digital wallets are morphing from credential vaults into active payment orchestrators.

THE GIMLET EYE Stablecoins—Or Tokenized Deposits?

2

TRENDS & TACTICS

4

The Business of Payments Isn't Technology

Wowed by new tech? Keep in mind it's the tech's potential to birth new business models that's paramount.

A Judge's Ruling Re-Ignites a Fierce Battle Over Interchange

The court expanded an existing injunction against an Illinois interchange cap to include credit unions.

Square Doubles Down on ISOs as a Sale Channel

The payments-tech giant is making a play for a sales model it shunned years ago.

Priority Announces It Will Go Private in a \$1.6 Billion Deal

The big processor hopes to reap more value for investors by ending a nine-year run as a public company.

Plus, Security Notes argues there's more to gain than to fear in AI, and Payments 3.0 warns time is running out on companies not prepared for agentic shopping.

E-COMMERCE

12

Stablecoins and Tokenized Deposits: How They Differ

There's been a lot of talk lately about tokenized deposits. They bear a strong resemblance to stablecoins, but they're not the same thing. Here's the scoop.



Photo: 123RF/uximetcpavel

ENDPOINT

25

Payments Under Pressure

The real test of payment infrastructure happens when millions try to pay at once. Here's what the world's biggest sporting events reveal about payment resilience.

STRATEGIES

22

Strategies for Revenue Protection, Part I

For transit agencies, preventing fare evasion and increasing revenue are key imperatives. In this first part of a two-part article, learn how experts are attacking the problem now.



Photo: 123RF/boy/iso

Photos: smartphone: shela051201/123rf.com; wallet and code generated by AI

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.

STABLECOINS HAVE BEEN grabbing the headlines lately in the payments business, but a related—and somewhat lesser known—technology may be gaining steam.

ACI Worldwide early last month said banks will be able to process payments via tokenized deposits as well as traditional payment methods through its move to add Swift ledger transactions to its ACI Connetic payments hub. Swift introduced its blockchain-based ledger last year.

Tokenized deposits are digital representations of commercial bank money entered on a blockchain or distributed ledger. They have some similarities to stablecoins, but are far from the same thing. ACI, one of the country's largest payments processors, introduced ACI Connetic last year. It combines card processing, account-to-account payments, and fraud prevention on a single platform.

ACI says its latest move will let banks process payments via tokenized deposits along with familiar payment methods with no change in operations, workflows, or technology. That means a separate operation for payments via digital assets is not needed, the processor says.

ACI Connetic will allow payments orchestrated through Swift's ledger to be managed alongside other payment flows within a common operation, ACI says. The company argues this versatility will grow in importance as trends such as digital assets become more pronounced and as payment methods such as tokenized deposits are emerging from pilots and entering production.

So what's so important in all this? Growth. Aaron McPherson, principal at AFM Consulting, told us that because "there is still a lot of manual labor and custom processing involved in tokenized-deposit transfers, adding this [new] support is necessary for the technology to be able to scale."

The ultimate objective now for ACI Connetic is to ease the way for banks to slide Swift ledger transactions into the same platforms they use for payments processing, according to ACI. For Swift, ledger transactions are real-time entries on a blockchain that banks can use to settle cross-border transactions with regulated digital assets.

Meanwhile, digital currency is only growing more prominent. SoFi Technologies Inc. and Mastercard said recently SoFi Bank is the first national bank to go live with stablecoin settlement for the bank's credit and debit card platform on Mastercard's global network. The integration uses the SoFiUSD stablecoin for settlement.

Utah-based SoFi Bank says it is committing the whole of its \$25-billion card program to settlement via SoFiUSD. The advantage of the program for merchants is that "businesses have faster access to their money via the speed of blockchain, with the safeguards of a bank," Anthony Noto, SoFi's chief executive, said in a statement released by the bank.

Speed is indeed of the essence. Are payments players ready for both of these technologies?

John Stewart, Editor | john@digitaltransactions.net

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

EDITORIAL ADVISORY BOARD
Eula L. Adams
John Elliott

Alex W. "Pete" Hart
Former Chief Executive Officer,
Mastercard International

William F. Keenan
President, De Novo Corp.

Dr. Gideon Samid
Chief Technology Officer,
AGS Encryptions Ltd.

DIRECTOR OF ADVERTISING
Robert A. Jenisch, 630-547-2887
bob@digitaltransactions.net

ADVERTISING SALES REPRESENTATIVES
Robert Mitchell, 630-547-2887, x7
bmitchell@digitaltransactions.net

Rob Akert, 630-547-2887, x6
rakert@digitaltransactions.net

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.

The views expressed in this publication are not necessarily those of the editors or of the members of the Editorial Advisory Board. The publisher makes reasonable efforts to ensure the timeliness and accuracy of its content, but is not engaged in any way in offering professional services related to financial, legal, accounting, tax, or other matters. Readers should seek professional counsel regarding such matters. All content herein is copyright © 2026 Boland Hill Media LLC. No part may be reproduced without the express written permission of the publisher. 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.





Ready to build and grow your business?

As a merchant acquiring partner, Merrick Bank delivers flexible payment solutions, tailored programs and trusted risk management expertise designed to help you scale with confidence.

Today, we support 100,000+ merchants and over \$60B in annual card volume.

- ✓ **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 dedicated to building a customized acquiring program and supporting you every step of the way.

Contact us

¹ by transactions

THE BUSINESS OF PAYMENTS ISN'T TECHNOLOGY

It's easy enough to be wowed by new technologies, especially those that may appear to promise new revenue for payments companies. But the real value of the technology is in the business models that form around it, says James Wester, director of cryptocurrency and co-head of payments at Javelin Strategy & Research.

Wester, speaking last month at the Western States Acquirers Association annual conference in Palm Desert, Calif., said every technology in payments follows the same arc. At first, it is unfamiliar and needs to be explained, then it catches the eyes of early adopters, spreads until it's expected, and finally turns into another cost of doing business.

Whether it's artificial intelligence, stablecoins, tokenization, or real-time payment rails, the early phases of awareness usually focus on the tech itself.

"This industry is particularly susceptible to this," Wester said, "because every year we have seen so many things come out." But those technologies that endure usually eventually become ordinary features.

"Many of the services now that we build businesses around, all had to be explained at one point," Wester says. "Every successful technology goes through a very familiar pattern. It begins with something new, it requires explanation. It becomes a slight advantage for some companies. [To reach] network effects, and we are a network industry, requires wide adoption before it really succeeds. Eventually, it's something that every provider has to include. And at that point, while the technology still matters, it stopped being the reason that your customer comes to you."

Wester says while new technologies may be enthralling, their true usefulness is on the business side. "Technology is here, but the business is on the other side. And that's ultimately what matters," he says.

Payments companies evaluating technologies, such as AI or stablecoin acceptance, should ask questions like: What problem does the technology really solve? Whose behavior has to change? "And again, the really important one, who's going to pay us for it?" he says.

Having a slick presentation deck and an interesting product may have appeal, but without supporting answers to those questions, a business doesn't exist, Wester says.

His analysis is affected by the economic backdrop merchants face. Consumer spending is holding up in terms of dollar value, but real spending has barely moved due to inflation, and businesses face rising

costs. In this environment, a sales pitch built on saving a few basis points in processing costs likely isn't enough to sway a merchant to pick a payment provider.

If technology can provide a value beyond that, and if it can remedy a problem the merchant needs to solve, it can be useful.

Wester's advice to acquirers and processors is to resist the urge to build a strategy around a technology's name. Instead, he suggests, find a merchant's actual costly problem, whether it's lost sales, slow settlement, or chargebacks, and work backward to the tools that solve it. Vertical

expertise is harder for competitors to replicate than access to any given technology.

"Don't build where there aren't economics," Wester says. "You don't get paid to be innovative. That's not what companies are paying you for."

—Kevin Woodward

A JUDGE'S RULING RE-IGNITES A FIERCE BATTLE OVER INTERCHANGE

A federal court ruling issued late last month has re-ignited a long-standing dispute over the question whether tips and tax can be exempted from the calculation of interchange merchants pay on credit card transactions in Illinois following that state's adoption in 2024 of the Illinois Fee Prohibition Act. The controversial act is expected to take effect July 1, 2027.

The ruling from judge Virginia Kendall of the Northern District of Illinois expands an existing injunction against the act to include national credit unions. National banks, federal savings and loans, out-of-state chartered banks, and card networks had previously been exempted by the injunc-

tion. State-chartered banks and credit unions remain subject to the act. Estimates indicate some 235 state-chartered banks and nearly 200 state-chartered credit unions operate in the state.

The move to exempt federal credit unions drew a strong rebuke from the Merchants Payments Coalition, a group that lobbies on behalf of retailers on payments matters.

"The NCUA has clearly exceeded its authority, and we expect the court will be overruled in an appeal or subsequent case," said Doug Kantor, an MPC executive committee member. "States can and should protect their local businesses and consumers from abusive, unfair practices by credit unions and

banks." Kantor is also general counsel for the National Association of Convenience Stores. The NCUA refers to the National Credit Union Association.

Interchange is the percentage of a card transaction merchants pay to issuing banks. The fee, typically around 2% to 3% of the sale, has grown increasingly controversial as merchants look to cut what they see as excessive transaction fees. Banks and interchange advocates argue the fee is necessary to cover the costs imposed by processing and expected risks.

Among avenues remaining for merchants opposed to Kendall's ruling is an appeal to the Seventh Circuit Court, of whose jurisdiction



Kantor: "The NCUA has clearly exceeded its authority, and we expect the court will be overruled in an appeal or subsequent case."

Kendall's court is a part, observers say. The MPC estimates the law will cut expenses for merchants in Illinois by some \$500 million a year.

At the same time, opponents of the IFPA, which include processors, banks, and lobbying groups, repeat their argument that the law dis-

torts the economics of card transactions, ultimately hurting cardholders. These parties say they seek full repeal of the law.

—John Stewart

SQUARE DOUBLES DOWN ON ISOS AS A SALE CHANNEL

Square is making a big play for independent sales organizations, a merchant-sales model it shunned 16 years ago in favor of direct acquiring. Square, the point-of-sale and acquiring unit of Block Inc., was one of the sponsors of the Western States Acquirers Association conference last month in Palm Desert, Calif. Mike Collins, Square's global head of resellers, also contributed to a panel on how merchant sales is evolving. Collins says the human aspect of merchant sales is foundational, but technology can lead the way. Square since its start in 2009 has been

mostly known for its direct-sales approach to acquire merchants. But in 2024 Jack Dorsey, cofounder of Square and head of its parent company Block Inc., said Square might enlist independent sales organizations to reach more merchants, a move it tried at its founding but determined it didn't produce expected results. After a subsequent launch of an ISO reseller program, Block said in May it had more than 140 participants. The human aspect may be important, but Collins says technology can help differentiate processors. "You have to lead with

technology," Collins told the WSAA attendees. Those organizations leading with technology are not just pitching a way to save a prospect a few dollars, he says, but they are actually bringing a solution that can help a business. Coming to a merchant with a benefit instead of a sole price message is indicative of a consultative sales approach, said Shawn Dalton, a panelist and senior vice president of Exectras. Exectras announced its Exectras Payments venture in September. "People do business with people they like and that human aspect of it," Dalton told attendees. Still, the rise of integrated point-of-sale platforms, such as those from Toast Inc., can be a force narrowing the window in which a sales agent controls the merchant relationship. A merchant using an integrated POS system may be a tougher sell because that system provides more business functions than payment processing. Any competitive system must produce what the merchant already gets and be different enough to warrant the switch. Some may turn to artificial intelligence as a way to stand out, but it may not do that in a way many may expect. It can be used for statement

MONTHLY MERCHANT METRIC

Chargebacks Transactions %

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**. For all industries including Higher Risk

Metric Definitions: (Only use definitions related to an individual month's release)
Chargebacks Transactions % of Transactions - Chargeback number divided by bankcard + OptBlue transactions

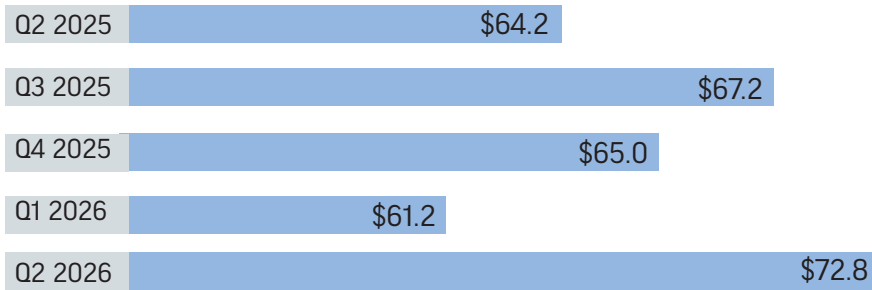
This report is based upon information we consider reliable, but its accuracy and completeness cannot be guaranteed. Information provided is not all inclusive. All information listed is as available. For internal use only. Reproducing or allowing reproduction or dissemination of any portion of this report externally for any purpose is strictly prohibited and may violate the intellectual property rights of The Strawhecker Group. ©Copyright 2026 The Strawhecker Group. All Rights Reserved.
DISCLAIMER: The Strawhecker Group (TSG) may not be endorsed, sponsored by, or in any other way affiliated with the any companies or their logos illustrated in this presentation. The trademarks shown are registered and their own. This document has not been prepared, approved, or licensed by any entity displayed.

Date	Chargebacks Transactions %
Q2'25	0.037%
Q3'25	0.044%
Q4'25	0.042%
Q1'26	0.041%
Q2'26	0.036%
Jul'26 (T3M)	0.036%



PAYMENT VOLUME REBOUNDS FOR SQUARE

(GPV in billions)



Source: The company

analysis, to generate sales presentations, and to provide 24/7 support in multiple languages, effec-

tively stripping out administrative friction and freeing up personnel to work on more complex issues.

As AI adoption accelerates within payments, the human element of the sale becomes more important, said Justin Vollrath, founder and chief executive of PayCompass, one part of the Exectras Payments venture.

“On the sales side, we’re looking at how we can use [AI] to just provide faster access to information,” Vollrath says. “Our goal is not to go away from that human interaction, but how can we make the human interaction faster, more efficient, and more effective.”

—Kevin Woodward

PRIORITY ANNOUNCES IT WILL GO PRIVATE IN A \$1.6 BILLION DEAL

An investor group led by Priority Technology Holdings Inc. chairman and chief executive Thomas Priore will take the processor private in a deal valued at \$1.6 billion, or \$8.05 per share in cash. The company’s closing share price on Sept. 25 was \$7.78.

The agreement follows a preliminary, non-binding proposal publicly disclosed in November. The deal, which will end the company’s nearly nine-year run as a public company, is expected to close in the first half of next year.

“After a comprehensive evaluation of the proposal, a rigorous valuation analysis, and extensive negotiations with Tom and his affiliates, we are delivering a transaction that provides compelling and certain value to Priority’s unaffiliated stockholders,” said Michael Passilla, chairman of a special

committee set up to review the transaction, in a statement.

“We believe this is the best path for the unaffiliated stockholders to realize the significant value from their investment in the company,” Passilla continued. Unaffiliated shareholders are those who do not have an executive role with the company, nor a controlling interest in it.

The committee, which was unanimous in supporting the deal, consisted of independent and disinterested directors, Alpharetta, Ga.-based Priority said. The group conducted a what Priority’s announcement said was a “robust” review of the transaction, relying on consultation with independent legal and financial advisors.

Priority, founded in 2005 by the brothers Tom and John Priore,

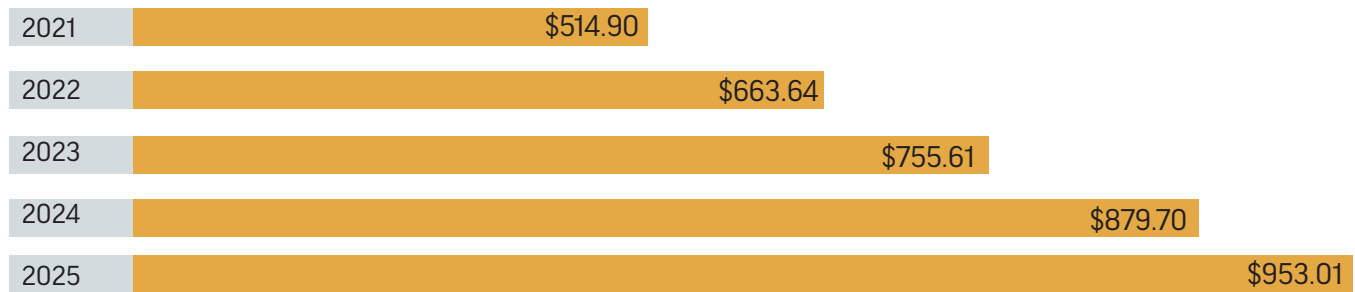
reported second-quarter revenue of \$262.3 million, up 9% from the same period last year, with an 8% increase in adjusted gross profit to \$99.9 million. Revenue for the first half of the year rose 10% to \$511.8 million, while gross profit hit \$198.7 million, up 11%.

Priority disclosed in November it had received a preliminary, non-binding take-private proposal from the investor group. At the time, the group proposed buying the shares it did not already own at a price ranging from \$6 to \$6.15 each, according to the company. The company’s announcement indicated Thomas Priore held about 58% of the company’s outstanding common stock.

Among its most recent deals, the company last month agreed to acquire Convenient Payments,

PRIORITY: REVENUE NEARLY DOUBLE IN FIVE YEARS

(in millions)



Source: ?????????

which does business as Intellipay, a privately held processor based in Draper, Utah, for \$11.5 million plus another \$3.5 million in earn-out payments over eight quarters following the close. The company at nearly the same time agreed to process ticket sales for the Tampa Bay

Buccaneers of the National Football League. That deal includes marketing rights that include branding in the stadium.

Priority has not been shy about expanding into new acquiring markets. It announced in October last year it had entered the market for

processing automotive-servicing payments with its acquisition of DMSJV LLC, also known as Dealer Merchant Services, a payments provider whose capabilities include surcharging to help dealers cover transaction costs.

—John Stewart

Digital Transactions News

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

Digital Transactions News is packed with news and information from the \$123.4 billion transaction industry:

- ▶ Two original stories every issue
- ▶ Trending stories, so you know what our subscribers are reading
- ▶ Links to Digital Transactions magazine
- ▶ Calendar of events
- ▶ **PLUS!** "In Other News" The most complete listing of announcements from the payments community

Subscribe today at Bolandhill.omed.com/dtr/ or email publisher Bob Jenisch at Bob@digitaltransactions.net

AI: IT'S ABOUT PROTECTING, NOT PANICKING

NOVELISTS AND science-fiction gurus have spun assorted scenarios for the demise of humanity at the hands of AI. This is because, unlike the nuclear threat which everybody understands (a very big boom!), AI is a conceptual mystery, breeding fear and panic.

Let's first remind ourselves that AI lives on the Internet. All that people have to do is to shut down the Internet to stop whatever AI may concoct. Of course, this will be a huge hardship for us, having lived so comfortably in cyberspace for quite some time. But if we properly prepare, we can meet this challenge. After all humanity survived very well without Internet for most of its history.

On the other hand, AI stands to disrupt electronic payments from the ground up, and that is not science fiction. AI quickly identified the top programmer in a large bank, and correctly assumed that he programmed his access with facial recognition only (to make things easy), not bothering with passwords and such. AI learned enough about this programmer, then offered him access to a very enticing Web site AI knew he would like. Entrance to this site required facial recognition.

There are plenty of such intrusions and they are done quickly. For large databases with many customers, the risk is very high. Once in,

BY
**GIDEON
SAMID**

gideon@bitmint.com



AI agents learn how to stay invisible. Is your bank unknowingly hosting AI agents? Defensive strategies are being developed. More in coming columns.

The most universal threat, though, lies in breaking encryption. Every mainstream encryption is readily breakable through brute force—the bad guys try all possible keys until they find the right one. So security designers make the number of keys so large it would take years to try, on average, half the number of keys. When humans try a key and it doesn't work, they drop it and randomly try the next key. AI, by contrast, gets the response for the wrong key and learns from it how to get closer to the right key.

Imagine you have 100 keys, but only one of them opens a given lock. You pick a random key, and if the lock doesn't open you toss it away and randomly pick another key, and so on until you open the lock. That is the "brute force" approach. On average, you will try 50 keys before you hit the right one.

However, an experienced lock picker evaluates how each wrong

key is stuck or moves in the lock, and learns from that what kind of lock it is, thereby making good guesses about which is the right key. He finds it, say, in seven trials rather than 50. This is "accelerated brute force"—the AI difference. Scary.

How advanced this accelerated brute-force strategy is, nobody reveals, but no mainstream cipher is resolutely protected. To stop this cipher-cracking AI, it is necessary to apply a different type of cryptography. Right now, that is virtually impossible. Cryptographers spent years refining the current approach to security. It is installed in countless protocols, and it runs on inertia. Secret security is another story. The AI stopper is something called "Non-Trivial Ciphertext." An example: the cipher BitFlip.

Submitting to the "AI-end-of-the-world" horror stories just drains efforts to fight back. Instead, we should focus on AI threats knocking on our door. A coming column will describe key strategies, like smart use of randomness. Randomness poisons AI. It's about disrupting longstanding relationships, making switches with no special reason, just to avoid durable routines, which AI builds on. It's also about keeping data out of reach for AI. DT

SO YOU THINK YOU'RE PREPARED FOR AGENTIC SHOPPING?

WILL THE ARRIVAL of shopping bots lead to a robot apocalypse for payments?

Agentic artificial intelligence is the next phase of online shopping. It is when shoppers empower an artificial-intelligence tool to make purchases on their behalf. So, a shopper asks a bot to go out online and find an item with a particular set of characteristics, maybe sets a price limit, and gives the bot a way to pay.

According to a survey by Visa, 55% of U.S. consumers are familiar with the idea of AI shopping assistants. The same survey found that saving money would be the top driver for using an AI shopping assistant.

This will cause headaches for payments providers, so they need to prepare now.

As people get ready for a time when they will turn shopping over to their computers, payments providers are working to keep up. For example, in April, Digital Transactions reported that American Express is releasing a software development kit called Agentic Commerce Experiences to help cardholders and merchants prepare for the rise of the shopping machines.

As we enter this new frontier, it is worth thinking about where the risks lie.

First, Agentic AI will lead to pressures on brand loyalty for both mer-



BY BEN JACKSON

bjackson@pa.org

chants and payments providers. As noted, shoppers intend to use Agentic AI to maximize savings. Maximizing rewards will follow naturally.

It is easy to imagine the user prompt: "Find me a pair of blue running shoes in my size at the lowest price possible. Make the purchase at the Web site with the lowest price using whichever card maximizes my rewards."

The merchant and the payments brands could lose out when the AI agent is tasked with minimizing costs and maximizing rewards, particularly if the agent is built by a third party. However, retailers and banks might use Agentic AI to build walled gardens.

If merchants build the bots, the internal logic of the bot might also keep the shopping in house and look for ways to minimize interchange. Bots built by a payments provider might look to maximize interchange or steer payments towards cards with high interest rates. Both of these moves may prompt action by regulators and legislators.

Another risk is fraud. Prompt injection attacks could steer an AI agent astray. Fraud rings might focus

on compromising shopping bots to steal credentials or have them shop for someone other than the user.

Then there is the risk of first-party fraud, where end users say the bot went rogue and made a purchase they should not be responsible for.

First-party fraud is already a problem for card issuers. In 2024, first-party fraud accounted for more than a third of all fraud globally, according to a Lexis Nexis report covered in this magazine. In January 2025, Digital Transactions reported that 13% of U.S. consumers committed first-party fraud during the 2024 holiday-shopping season. It is safe to say these were not people blaming AI agents for going rogue, but that excuse likely will come into play as the use of shopping bots grows.

Dealing with these issues is going to be a challenge for merchants and payments providers. In May, the U.S. Payments Forum released a meeting summary that said the key is going to be figuring out how to "capture and preserve consumer intent throughout the transaction lifecycle..."

Payments providers and retailers should begin gaming out the possibilities created by this new technology. They should consider what their current capacities are to respond to the risks and opportunities and what kind of tools they will need in the fast-approaching future. **DT**

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.



THE COMPANIES OF GENERAL CREDIT FORMS

GCF
GENERAL CREDIT FORMS, INC.



PSI
Paper Systems
INCORPORATED



South Seas Data LLC

.....
www.gcfinc.com • (888) GCF-NEWS

STABLECOINS AND TOKENIZED DEPOSITS: HOW THEY DIFFER

There's been a lot of talk lately about tokenized deposits. They bear a strong resemblance to stablecoins, but they're not the same thing. Here's the scoop.

BY **AARON MCPHERSON**

Aaron McPherson is principal at AFM Consulting Partners.

IF YOU HAVE been reading the trade press in 2026, you have seen the term “tokenized deposits” a lot. Some people use the term “deposit tokens,” which is much the same thing. You may have just gotten your head around stablecoins. Now here is a new kind of token. What is it? And why is it suddenly such a big deal?

This article is a quick guide. It explains what tokenized deposits are and how they compare to stablecoins.

TWO KINDS OF DIGITAL DOLLAR

Both kinds of token look the same on the surface. You hand over a dollar. You get back one token worth a dollar. Return the token, and you get your dollar back. Both are issued one for one. The difference comes with what happens to your dollar after that.

A stablecoin issuer has to park it. The GENIUS Act, which became U.S. law in 2025, says the issuer must hold safe assets equal to every token it has sold. The list of such assets is short: cash, bank deposits, and short-term Treasury bills. The issuer must keep those assets apart from its own money. And it may not lend them, pledge them, or put them to work. The law also bars the issuer from paying any interest.

A bank does not park your dollar. It mixes it with the rest of its deposits and sends it out the door as a loan. Your token is a claim on the bank, not a claim on a pile of set-aside cash. This is a little less safe than a stablecoin, but safe enough for most purposes.

Parking money is fine for a cryptocurrency firm like Circle or Tether. Issuing tokens is their



Photo: 123RF/boyloso

business, and they earn their profits on the yield from the assets in the pile. Banks, however, earn money by lending. This is the engine of the entire economy. When a bank lends, it creates new money, which helps the economy grow.

Deposits already have clear rules. Regulators know how banks take deposits, how much capital they must hold, and how to check for money laundering. A tokenized deposit is the same old liability, just recorded in a new place. With stablecoins, though, many of the rules are still being written.

A stablecoin is a bit like digital cash. Anyone with a crypto wallet can hold it and trade it. A tokenized deposit, on the other hand, is a claim on a specific bank. Sending it to a customer of another bank is a little more complicated than with stablecoins. The two banks need a way to exchange cash to keep things in balance. One proposed solution is the exchange of central-bank reserves.

On the plus side, a tokenized deposit may be covered by deposit insurance. A stablecoin is not. You have to trust that the issuer really has the reserves to back its stablecoin.

WHAT THEY HAVE IN COMMON

Both kinds of tokens live on a blockchain. That brings the same benefits to both:

- **Transparency.** Every transfer is recorded. You can trace where the money came from. That makes it harder to launder money or dodge sanctions.
 - **Finality.** Once a transfer is recorded, it is done. Refunds have to be made as new transfers. (Issuers can still freeze or claw back tokens in some cases).
 - **Atomic settlement.** With a conventional transaction, a payment has two steps: the instruction and the settlement. On a blockchain, these steps happen at once. Smart contracts can swap money for goods, or one token for another, in a single step. If one side fails, nothing moves. This is called “delivery versus payment” or “payment versus payment.” It removes the risk that one side will not deliver.
 - **Always on.** A blockchain never closes. There are no batch windows, no cutoff times, and no business hours. Customers can pay 24/7.
- **Fewer middlemen.** Two parties can trade directly on the chain. No long chain of go-betweens is needed. Smart contracts enforce the rules. Each layer you remove cuts cost.
 - **Better use of cash.** Today, firms park money in reserve accounts to cover the day’s payments. With tokens, they can move money just in time. The rest can be put to better use.
 - **Tiny payments.** A token can be split into very small pieces. Circle’s USDC stablecoin, for example, goes to six decimal places. That makes it possible to pay a fraction of a cent for one news article, or one query to a data service. This matters more as AI agents start to shop and pay on our behalf. Tokens are digital and secure by design, so they are a natural fit.

So why aren’t we using them yet? The first reason is plumbing. The old financial system and the blockchain world have to be connected. We do not yet know if tokens can handle the volume of commercial trade. Working at scale requires a lot of automation, and all of that has to be built and tested. Banks



McPherson: For tokenized deposits to flourish, “the old financial system and the blockchain world have to be connected.”

are still in the pilot stage with this.

The second reason is regulators. Banks do not want to get too far ahead of them. On a recent panel, a speaker put it this way: "Own what you can explain to your regulator." The GENIUS Act made the U.S. much friendlier to tokenized money. Even so, no bank wants a regulator to second-guess its decision to scale up.

The third reason is privacy and fraud. Recording every payment forever sounds great. Then you realize this means others can see

how you spend your money. Deciding what goes on the chain, and in how much detail, is still an open question.

Fraud is a problem, too. As with all real-time payments, banks lose the lead time they have had with batch systems to spot fraud. New tools are needed. And since transfers are final, a fraudulent payment is hard to undo.

THE BOTTOM LINE

Tokenized deposits and stablecoins

are two versions of one idea: putting money on a blockchain. The big difference is what the issuer may do with your dollar. A bank can lend against a tokenized deposit and pay interest on it. That keeps the current banking model intact. On the other hand, a stablecoin ties up the dollar, which could undermine the banking system by siphoning off deposits.

That's why most financial institutions prefer tokenized deposits. They reinforce banks' existing business rather than undermining it. **DT**

Co-Branded E-Mail Marketing

Get the Results You Need

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.

**To get started, contact
Publisher Bob Jenisch today:
877-658-0418 | bob@digitaltransactions.net**

THE ONLY MAGAZINE COVERING THE TOTAL PAYMENTS MARKET

In 2019, there were 150.2 billion digital transactions in North America.

Digital Transactions magazine covered them all.

It is the only publication addressing the total market.

Financial institutions, independent sales organizations (credit and debit ISOs, ATM deployers and value added resellers), processors, along with the top tier retailers all turn to *Digital Transactions* for the trends affecting the payments market and, more importantly, their livelihoods.

Covering the electronic payments business for 18 years, *Digital Transactions* magazine is your independent source for changes affecting the payments market. *Digital Transactions* is also available in a digital edition on our web site, DigitalTransactions.net

Subscribe today by going to Bolandhillmeda.com/dtr/ to start tackling the ever-changing payments market.





Say Goodbye to the Passive Wallet

**Digital wallets are morphing from credential vaults
into active payment orchestrators.**

By Kevin Woodward

Consumers of a certain age know well how many steps were required to take a picture. The first step was to load the film. The photographer had to set the exposure so the image wasn't too bright or too dark. That done, she had to point the camera and focus. The latter two steps could take seconds to complete.

Now, all of these steps have been compressed into simultaneous actions within a smart phone. One tap is all it takes.

Something similar is happening with digital wallets on smart phones. It may not be everywhere yet, but the days of mobile wallets identifying a user, authenticating the individual's permission to pay, and authorizing a transaction all in one step are fast approaching. The collapse of three actions into one is at hand.

At the base of this transformation is the spread of tokenization. Debuting in 2014, network tokens made possible mobile payments using a smart phone. Without a way to switch out the actual credit or debit card number for a stand-in string of data, mobile wallets could have languished. Now, network tokens permeate the payments industry and extend well beyond their original use in mobile payments.

"For any merchant with a concept of a user account, tokenization isn't optional any more. It's essential," says Elijah Murray, global chief technology officer at Digistore24 Inc. St. Petersburg, Fla.-based Digistore24 is an e-commerce platform.

"However, scope of use is now expanding beyond just the card," Murray says. "For example, if we offer instant bank payments in the U.S., we can tokenize the buyer's chosen bank account after their first payment and reuse it for future purchases without putting them through bank auth again."

"The same logic applies to Apple Pay and Google Pay," he adds. "Whichever service tokenizes the wallet knows which underlying card the buyer used, so we can surface that card to them before checkout instead of leaving them to guess what's behind the wallet icon, removing friction and increasing conversion."

Others see a similar evolution, with tokens as the foundation.

"Checkout is collapsing from a multi-screen, manually entered process into a single authenticated event," says Keith Riddle, chief executive of Payfinia, a Portland, Ore.-based payments provider.

Tokens' Crucial Role

It works like this. A user double clicks a side button, such as the one on the iPhone, to authenticate himself with a biometric enabling the device to unlock the secure element where the tokenized payment data is stored. By holding the phone near a point-of-sale terminal with NFC, the data are read and the success or failure of the transaction is relayed back to the user's mobile-device display.

"Network tokenization is the foundation," Riddle says. "Rather than passing raw [primary account numbers], wallets like Paze resolve a consumer's identity at the issuer level and return a network token bound to that verified relationship." Early Warning Services LLC's Paze is a bank-based digital-wallet service for online transactions.

"Because Paze is built on the issuer's existing cardholder data, the identity assurance and the payment credential arrive together. The merchant never sees or stores the card number, and the issuer's KYC work is effectively reused as the identity signal," Riddle continues. "The protocol has shifted from 'prove the card is valid' to 'prove the person is who the issuer already knows them to be,' with tokenization carrying both facts in one exchange."

Push provisioning can help issuers differentiate themselves from competitors, says Heather Spence, director of digital product development at CPI Card Group Inc. "Consumers increasingly expect to be able to get their payment credentials into a mobile wallet quickly," Spence says.

With that provisioning service as an aid, Spence says mobile-wallet use will continue to grow. “Issuers that continue treating push provisioning as a future-year priority risk falling behind fintechs and neobanks that make getting a payment credential into a mobile wallet one of the first things a customer can do after opening an account,” she says.

Migration to a unified checkout, with digital wallets central to the experience, is coming. “The industry is moving toward a checkout experience in which the wallet can confirm both who is initiating a transaction and which payment credential has been authorized, without requiring the consumer to repeatedly enter sensitive information,” says Louis Hoch, chief executive of payments provider Usio Inc.

“Tokenization is central to that model because the merchant can receive a transaction-specific credential rather than the consumer’s underlying card or bank-account details,” Hoch adds.

‘The Same Ceremony’

Other necessary elements are in place, too, in the form of standards and protocols.

Vanessa Grellet, managing partner at Arche Capital, a venture-capital firm, says the technology to enable a browser-based checkout experience is here in the form of the W3C Digital Credentials API. That is a Web platform standard that lets Web sites request, present, and issue digital credentials directly inside a Web browser.

Grellet says this standard is now shipping in more recent versions of Chrome, Google’s browser, and Safari, the Apple browser. It lets a merchant request

a verifiable credential directly from the device wallet, she says.

“Government ID, age attestation, a payment credential. No custom QR [code] scheme, no deep link, no redirect,” Grellet says. “The consumer consents once on-device, and the merchant receives a cryptographically signed payload rather than a photo of a license and a 16-digit card number.”

Other protocols are in place at the network level—click to pay is in use by all four U.S. card brands—and at the standards layer. “Network tokens protect the underlying card credential, while biometric and delegated authentication allow a trusted wallet or merchant to vouch for the customer,” says Advait Sinha, global head of payments at Nuvei Corp.

“Protocols such as click to pay show how these capabilities can come together to create a faster, more secure experience wherever customers pay.” Click to pay, launched by American Express Co., Discover, Mastercard, and Visa in 2019, is a one-click checkout service.

EMVCo is working on a Digital Payment Credential, a form of verifiable digital credential for payment card-specific applications. Some common verifiable digital credentials already in use are digital driver licenses, proof of age, and identity cards.

Regulators also are a factor, Grellet says. In the European Union, each member state has to provide at least one certified EU Digital Identity Wallet by December. The goal is to provide a private and secure digital identification for EU citizens, residents, and businesses to store, share, and sign digital documents, the European Commission says. Regulated parties must accept it by December 2027.



Spence: “Issuers that continue treating push provisioning as a future-year priority risk falling behind fintechs and neobanks.”



Riddle: “Network tokenization is the foundation.”

“Under that framework, identity proof and payment consent become the same ceremony—the wallet presents a credential that satisfies both requirements at once,” Grellet says.

Issuers and Merchants

With protocols and standards in place or under way, getting merchants and issuers onboard is critical. For many, that may require a shift in their approaches to fraud, identity, authentication, and payments.

It means thinking of them as one puzzle and not separate parts of the journey, says Dany Naigeboren, senior director for risk at Forter Inc., a fraud-prevention firm. “Fraudsters made that shift years ago, mapping everything from loyalty to returns for wherever value can be extracted. Hardening checkout alone just moves the pressure somewhere less defended,” Naigeboren says.

Merchants will need the infrastructure that preserves and shares identity and transaction data while maintaining flexibility across processors, payment methods, and tokens, he says. “Several standards are competing, and none has clearly won, so flexibility matters more than usual.”

Issuers need to be concerned with context and enrollment. “Richer signals mean better authorization decisions with less friction. And provisioning is where trust gets set: issue a credential to the wrong person and every merchant downstream inherits that mistake,” Naigeboren says.

The issuer role is just as important as merchant acceptance and developing the necessary rails. It can be straightforward for issuers, says Elana Golub, director

of product strategy at Method Financial, an Austin, Texas-based financial technology provider.

“They need to make it easy for consumers to add their cards to digital wallets; otherwise they risk losing out on wallet share in digital transactions,” Golub says. “This has more implications for their legal and regulatory teams than their technical ones, as the tactical changes require embracing consumer-permissioned data sharing as a distribution channel.”

Riddle suggests issuers change how they treat wallets, going from a card-on-file utility to a customer-facing extension of their identity franchise. It can be a key component of the relationship between the consumer and the issuer.

“The FI that authenticates the consumer owns the relationship,” Riddle says. “Merchants should prioritize wallet acceptance that reduces friction and fraud simultaneously, rather than treating each new wallet as another button. Adopt network tokenization, provision cards into wallets like Paze at issuance, ensure clean cardholder data for identity resolution, and instrument checkout to accept token-plus-identity in one call.”

Who are the Users?

Who these consumers are is another consideration. Some may assume only younger consumers are apt to use a converged digital wallet. Grellet says the growth is structural, not a fad of youth, though younger cohorts raise the ceiling as they take a larger share of total spend.

“Digital wallets accounted for 56% of global e-commerce transaction value and 33% of in-store spending in 2025,” she says. “That is from Worldpay’s latest Global Payments Report, covering 63,000 consumers across

42 markets. The market was valued at roughly \$57 billion in 2025 and is projected to reach \$68 billion this year—a nearly 20% year-over-year increase.

“By 2030, forecasts put it at \$145 billion, growing at about 21% CAGR,” she continues. “Juniper Research projects global wallet users will go from approximately 4.5 billion to 6 billion over the same period.”

Others agree that overall digital wallet use is going to increase, but as younger generations enter their higher earning years, that will produce a steady and consistent uptick over time, rather than a concentrated surge, says Guru Sahajpal, industry lead for financial services and fintech, at Teaneck, N.J.-based Cognizant.

“Under-25 shoppers already lead older generations in wallet adoption and usage. As these shoppers move into peak earning years, they continue the habit and spend more while doing it,” Sahajpal says. “That is the growth engine in my view. Not so much the headcount entering the workforce in any given year but rather the increase in spending power of people who already default to wallet use.”

For context, there are approximately as many as 66 million adult U.S. residents in the Baby Boomer segment, and a near equal amount—65 million—in Generation X. There are many more in the younger segments with 74 million Millennials and 72 million in Generation Z. Birth years range from 1981 to 2012 for the latter two.

On the identification front, a wallet’s value for identity authentication depends on how securely it is bound to the user and the device, how the credentials are issued and verified, and how account recovery is protected, says Ashish Jain, chief technology officer at OneSpan, a specialist in digital identity and anti-fraud services.

“Wallets are ultimately just one part of a modern identity-security posture. They need to work in tandem with passkeys, digital credentials, device intelligence, and transaction-level risk signals to provide the right level of assurance for each payment,” Jain says.

“Passkeys are one enabler, with 90% of individuals aware of the technology, standardized by the FIDO Alliance,” he continues. “At least 75% of [those aware] enabled a passkey on at least one account, FIDO research finds.”

The Centrality of Cards

On the flipside, though, is that bundling so much into one device or service could make it a single point of failure, Sahajpal says. “If it authenticates identity and authorizes payment, compromising it is worth more to a bad actor. So the same consolidation that makes authentication stronger also raises the stakes on securing the wallet itself, and that’s a balance the industry has to get right,” he says.

The advent of a consolidated experience involving digital wallets also could affect guest checkout, an online retailer’s utility for consumers not wishing to create a permanent account. Grellet says guest checkout should not be viewed as part of a growth strategy. She says Visa data highlights that manual guest checkout use fell from nearly 50% of online transactions in 2019 to 16% in 2025.

Riddle says guest checkout exists because entering card data in a form is tedious. “A wallet that authenticates in one tap removes the reason it exists,” he says. “The physical card becomes one form factor among



Hoch: “The industry is moving toward a checkout experience in which the wallet can confirm both who is initiating a transaction and which payment credential has been authorized.”



Grellet: “Identity proof and payment consent become the same ceremony—the wallet presents a credential that satisfies both requirements at once.”

several rather than the credential itself, and what persists is the issuer-verified identity underneath.”

Even if digital wallets have greater use, the card itself, with its PAN, expiration date, and verification code, will remain central to the wallet’s payment function.

“While the physical credit card may be leaving the checkout page, the card isn’t leaving the transaction. U.S. consumers still put well over \$15 trillion through cards

last year, and most wallet transactions are card funded regardless of what the shopper taps,” Naigeboren says.

In a card-led market, such as the U.S., wallets are still mostly card funded, Grellet says. “The rail persists. The presentation layer changes, but the funding source does not.”

The wallet may be doing more of the talking, but for now, the card is still footing the bill. **DT**

Get the latest news impacting the **payments market**

Today and every day follow
DIGITAL TRANSACTIONS
@DTPAYMENTNEWS on X

Do not be left behind.

Follow Digital Transactions on X,
formerly known as Twitter
@DTPaymentNews



STRATEGIES FOR REVENUE PROTECTION, PART I

For transit agencies, preventing fare evasion and increasing revenue are key imperatives. In this first part of a two-part article, learn how experts are attacking the problem now.

BY **AUDREY DENIS**

Audrey Denis is director of new ventures at Cubic Transportation Systems.

U.S. TRANSIT AGENCIES are facing a challenging budget environment, and many are in a position where they need to protect every dollar possible, especially the revenue brought in from fare collection.

As federal government-allocated budgets are set to dry up soon, fare collection will become a bigger source of operating income for agencies. That makes revenue protection a top priority for transit-agency decision makers. Alongside their partners, agencies are working to address revenue loss

through a combination of policy, technology, and enforcement.

Collectively, agencies across the largest metros lose millions of dollars of revenue due to fare evasion and fraud each year. New York City's Metropolitan Transportation Authority alone reported losing about \$600 million to fare evasion in 2022.

As balancing access and fare evasion becomes even more critical to their success, transit agencies are starting to look toward their payment-system partners for greater support in boosting their strategies.

There are three strategies that this article will cover over two parts:

1. Increasing payment options and lowering barriers;
2. Prevention of fare evasion;
3. Reduction of fraud

This part will cover increasing revenue and preventing fare evasion. Part two will dive exclusively into fraud reduction as it is a burgeoning topic that's relying on innovative solutions to deliver an answer.

WHO SKIPS OUT?

The fact is that the majority of riders pay their fare. It's a small group



Photo: 123RF/uximetcpavel

that creates challenges for agencies, but the impact of that group is significant.

One thing we've learned from working with agencies is that there isn't just one type of fare evader. Instead, we see four main personas:

- **Opportunistic** riders view fare evasion as a low-risk shortcut. It's often impulsive, driven by the moment. Visible enforcement and well-designed gates can act as deterrents;
- **Frustrated** riders feel dissatisfied with the service or perceive unfairness. For these riders, improving the customer experience and making the payment process more transparent can go a long way;
- **Economically** stressed riders sometimes evade fares because they don't have another option. Connecting reduced fares directly to payment credentials ensures these riders get the benefits they deserve without resorting to evasion;
- **Determined** riders are habitual or rebellious, sometimes driven by seeing others get away with it. Stronger gates, targeted enforcement, and visible signals when fare evasion is detected can help reduce their impact.

ENCOURAGING PAYMENT

Regardless of motivation, the most effective way to reduce fare evasion is to make paying as easy as possible. Many agencies are implementing account-based systems and fare capping to ensure riders always pay the best fare. Fare caps incentivize riders to never miss their payment in order to take advantage of the savings potential. This is particularly effective in dissuading frustrated riders from fare evasion.

Account-based ticketing opens the door to more flexible pricing and customer-focused initiatives. Fare capping, loyalty programs, and partnerships with employers or universities can encourage additional trips while maintaining revenue integrity. Off-peak discounts or special pricing promotions can help boost ridership during slower periods. All of this can be achieved with the right technology infrastructure in place.

It's also important to make reduced fares easier to access for those who need them. By tying discounts to both open- and closed-loop payment credentials, riders who qualify can automatically receive the correct fare. This not only supports equitable access but also removes one of the barriers

that sometimes leads to fare evasion, particularly for the economically stressed persona.

INCREASING REVENUE STREAMS

Revenue protection isn't just about minimizing losses. It's also about creating opportunities to grow ridership and payments.

A recent example of this approach is New York City's rollout of OMNY student transit cards in September 2024. These cards replaced the more restrictive MetroCards, expanding student travel benefits from three rides a day on school days to four rides a day, year-round.

The change makes the system easier to use and more appealing for students, while introducing them to OMNY's tap-and-go system early. The Metropolitan Transportation Authority (MTA) has been explicit that the goal is not only to support student mobility but also to convert school-pass users into regular paying customers over time.

Data plays a central role in making these efforts successful. Agencies can track the real-time impact of these programs, identifying when and where ridership changes and how it affects revenue. This allows them to adjust strategies quickly,



Denis: "Protecting fare revenue is a shared responsibility. It takes coordination between transit agencies, technology providers, enforcement partners, and payment networks."

ensuring incentives deliver the intended results without undermining overall fare collection.

IDENTIFYING FARE EVASION

When it comes to non-payment by those opportunistic and determined riders, agencies struggle to identify where and when fare evasion occurs. Traditionally, many have relied on manual surveys, sending staff into the field to observe and record incidents a few times a year. These surveys are time-consuming, prone to error, and provide only limited snapshots of activity.

To address this, agencies are turning to data-driven tools such as machine vision and AI. These technologies analyze fare-gate and bus-boarding activity, camera feeds, and tap data to pinpoint problem areas, identify trends, and

measure how fare evasion changes over time.

With these insights, enforcement resources can be deployed more strategically. Specifically, they enable focusing on areas with the highest potential for impact rather than spreading efforts evenly across the system.

Fare gates themselves are also evolving as part of enforcement strategies. Enhanced designs, coupled with visual and audible alerts when fare evasion is detected, create a visible deterrent. For opportunistic and determined fare evaders in particular, this kind of immediate feedback makes evasion riskier and less appealing.

COLLABORATION IS KEY

Protecting fare revenue is a shared responsibility. It takes coordination

between transit agencies, technology providers, enforcement partners, and payment networks to build systems that are accessible, secure, and effective.

Agencies benefit not just from the tools they implement but also from shared knowledge across the industry. By learning from one another, agencies can adopt strategies that have been proven successful and avoid common pitfalls.

There's no one-size-fits-all solution to fare evasion. The most effective approaches combine thoughtful policy, easy-to-use technology, equitable fare structures, and smarter enforcement. With this mix in place, agencies can reduce leakage, build trust with riders, and ensure more revenue goes toward maintaining and improving service. DT

Co-Branded E-Mail Marketing

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.

Get the Results You Need



It's really that easy!

To get started, contact Bob Jenisch today.

877-658-0418 | bob@digitaltransactions.com

It's crucial that
technology simply works.

endpoint

PAYMENTS UNDER PRESSURE

The real test of payment infrastructure happens when millions try to pay at once. Here's what the world's biggest sporting events reveal about payment resilience.

BY JEAN-PHILIPPE NIEDERGANG

Jean-Philippe Niedergang is acting group chief executive and EMEA-PACIFIC-LATAM chief executive at Castles Technology.



WE ONLY REALLY notice payment infrastructure when it stops working.

For most of the year, the systems that let us tap a card, scan a phone, or pay at a self-service terminal quietly do their job in the background. Few people give much thought to the technology behind those transactions because, when everything works, it is effectively invisible.

Then comes the real test. The referee blows a whistle for half-time and tens of thousands of supporters leave their seats at exactly the same moment, heading for food concessions, merchandise stands, transport links and vending machines. Within a matter of minutes, thousands of transactions need to be completed quickly, securely, and without interruption.

That is when payment infrastructure proves whether it has been designed for the real world.

Few events place greater pressure on payment infrastructure than the world's biggest football (soccer) tournament. It is estimated the tournament generated more than \$40 billion (U.S.) in economic impact across North America, while attracting record-breaking

television audiences across the globe. Every match creates thousands of simultaneous payment moments across stadiums, transport networks, and retail environments, all of which have to work without interruption.

That scale matters because this is not really a story about football. It is about what happens when extraordinary numbers of people converge on the same place, at the same time, wanting to do exactly the same thing.

They buy food and drink, pick up merchandise, pay for parking, use public transport, and visit self-service kiosks, often within the same few minutes. Every one of those transactions depends on technology that most people never notice unless something goes wrong.

THE REAL DIFFERENTIATOR

The payments industry has spent years improving speed, expanding payment choice, and creating smoother customer experiences. Those things still matter, and they always will. Increasingly, however, the more important question is whether the technology underpinning those transactions

can cope when demand spikes harder and faster than anyone anticipated.

Major sporting events simply make that challenge impossible to ignore. The same pattern plays out everyday in airports, transport hubs, music festivals, exhibition centers, and busy retail environments. The locations change, but the operational challenge remains remarkably similar. Large numbers of people arrive together, expect to pay immediately, and have little patience for delays. Forget customer experience, this is now an operational resilience issue.

This is where unattended payment infrastructure demonstrates its real value. A staffed checkout can often recover from disruption. A member of staff can explain the problem, try another payment method, or direct customers elsewhere. An unattended terminal has no such luxury. If the payment fails, the transaction fails.

That is why unattended environments demand a different level of resilience. The hardware has to perform consistently under sustained demand, while software must remain responsive during periods of exceptionally high transaction volumes. Every component needs to keep working when thousands of people are trying to complete a purchase within minutes rather than hours.

ADVERTISER INDEX

Digital Transactions

Pages IFC, BC, IBC, 8, 14, 15, 21, 24

General Credit Forms, Inc. Page 11

Merrick Bank Page 3

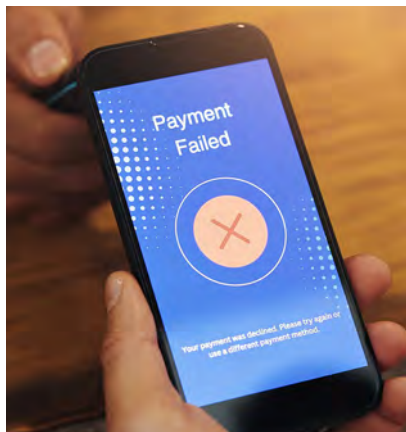


Photo: 123RF/peopleimages12

The industry has spent years solving these challenges across vending, transport, self-service retail and other unattended environments. Major sporting events simply compress those same operational demands into an incredibly short window, making them far more visible than they are during everyday trading.

THE BUSIEST MOMENT

Too often, payment infrastructure is evaluated against average trading conditions. In reality, the true measure of any payment deployment is how it performs during its busiest few minutes. Can operators monitor an entire fleet of devices in real time? Can software updates be deployed remotely when required? Can terminals continue processing transactions reliably as volumes surge? Most important, can issues be identified and resolved before customers even realize there's a problem?

These are increasingly the questions that separate resilient payment infrastructure from systems that perform well only under normal operating conditions.

Resilience also needs to be designed into the infrastructure

long before those peak moments arrive. That means thinking beyond the individual terminal and considering how an entire payment estate is connected, monitored and managed. As self-service environments grow, operators need visibility across thousands of endpoints and the ability to respond quickly when conditions change. Open, software-driven platforms can make that estate easier to manage, allowing functionality to evolve without repeatedly replacing hardware in the field. The objective is to build payment infrastructure capable of anticipating pressure and adapting before disruption reaches the customer.

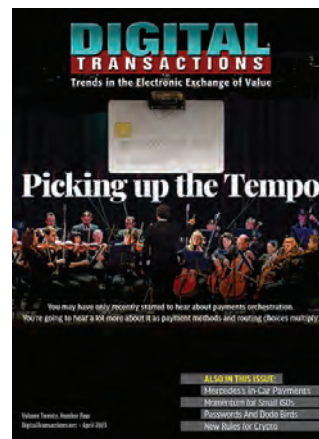
This summer's global football tournament offers one of the clearest demonstrations of what resilient payment infrastructure looks like under pressure, but the lesson extends well beyond football.

As commerce becomes increasingly self-service, connected and unattended, resilience will become every bit as important as speed, convenience, and payment choice. Whether it is a stadium, a railway station, an airport, or a retail environment during peak trading, the expectation is exactly the same. Payments should work, every time.

Customers rarely remember a payment that works exactly as expected. But they always remember one that does not. So the real measure of payment infrastructure is what happens when millions of people decide to pay at once. That is when resilience becomes visible. It is also the moment modern payment infrastructure is built to handle. **DT**

THE ONLY MAGAZINE COVERING THE TOTAL PAYMENTS MARKET

In 2022, there were 170.3 billion digital transactions in North America. *Digital Transactions* magazine covered them all. It is the only publication addressing the total market.



Financial institutions, independent sales organizations (credit and debit ISOs, ATM deployers and value added resellers), processors, along with the top tier retailers all turn to *Digital Transactions* for the trends affecting the payments market and, more importantly, their livelihoods.



Covering the payments business for 20 years, *Digital Transactions* magazine is your independent source for changes affecting the payments market. *Digital Transactions* is also available in a digital edition on our web site, DigitalTransactions.net

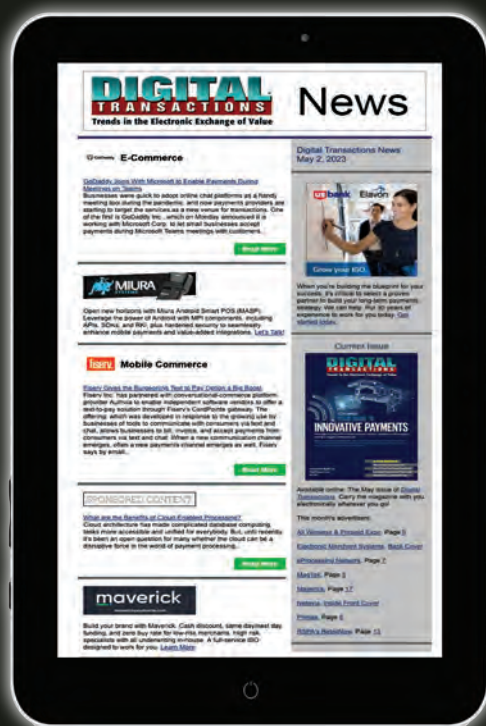
Subscribe today!

Visit Bolandhillmedia.com/dtr
to start tackling the ever-changing payments market.



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