DIGITAL TRANSACTIONS®
Trends in the Electronic Exchange of Value



50 WAYS TO LEAVE MAGSTRIPE

General purpose cards long ago moved to chip.
Now, EBT/SNAP cards are doing so, but in 50 different ways.

ALSO IN THIS ISSUE:

AmEx's Next Step
Learning to Love AI
Confronting Fare Fraud
Getting AI Tech Right

Volume Twenty-three, Number Eight
DigitalTransactions.net
November 2026

globalpayments





Mark your calendar: new webinar

From agent to growth leader: How MPI built a 3,000+ merchant services business

Date: Wednesday, December 9, 2026

Time: 11:30 am ET/8:30 am PT

Featuring Kyle Morgan, Founder & CEO of Mercantile Processing Inc.

You know how to sell. But do you know how to scale?

Find out what it really takes to grow from independent sales agent to full-service provider in this exclusive fireside chat.

Your ISO growth playbook is waiting.

Register today

https://bit.ly/4sfBA7z

> **When we made the decision to go full-service, Global Payments was there to provide the resources and support we needed. It was a very smooth transition, and we felt ready to swim within 30 days."**
>
> **Kyle Morgan**
>
> MERCANTILE PROCESSING INC.

©2026 Global Payments Inc. All trademarks and service marks contained herein are the sole and exclusive property of their respective owners.

contents

NOVEMBER 2026 • VOLUME 23, NUMBER 8

50 Ways to Leave Magstripe 16

General purpose cards long ago move to chip. Now EBT/SNAP cards are doing so, but in 50 different ways.

THE GIMLET EYE Back to the Drawing Board on Interchange 2

TRENDS & TACTICS 3

AmEx's Next Step for Agentic Commerce

The network hopes its recently introduced framework for agentic commerce will take its place as part of a payments standard.

Mastercard, Visa, And Stablecoins

Both networks are steadily moving the crypto towards the mainstream. Here's why.

Marqeta And Coinbase Have Their Say

The two companies are working towards cards customers can use to tap their stablecoin balances.

AI's Impact on Fraud Rates—And Fraudsters!

Meet the AI-fluent fraudster. He could be your next-door neighbor.

Plus Security Notes shows how to thwart hackers tempted to hijack AI agents, while Payments 3.0 details the power of financial-institutions charters when it comes to interchange.

STRATEGIES 12

When Something Else Spends Your Money

Governance and risk management will be necessary in the agentic era, and will likely be tested in novel, challenging—and unpredictable—ways.



Photo: 123RF/pitinan



Photo: 123RF/grispb

STRATEGIES 22

Strategies for Revenue Protection, Part II

Last month, we looked at payments lost to fare evasion in mass transit. Now, it's time to examine the threat of fare fraud and how to confront it.

ENDPOINT 27

Fragmented Tech Is Reshaping AI Economics

In business, getting AI right is critical. In restaurants, the stakes have never been higher.

Photo: 123RF/liudmilachernetska

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

BACK TO THE DRAWING BOARD ON INTERCHANGE

WILL THE CONTROVERSY swirling around interchange never cease?

A federal appeals court has required the Federal Reserve to rewrite the key interchange limits included in the Fed's controversial (to say the least)15-year-old debit card rule. This outcome came in a federal appeals court decision last month that struck down the cap on interchange the Fed established way back in 2011.

So what gave rise to this sweeping outcome? A ruling by a three-judge panel of the U.S. Circuit Court of Appeals for the 8th Circuit upheld a challenge brought by a North Dakota truck stop and c-store operator called Corner Post, which challenged the Fed's 21-cent debit-interchange cap as too high in light of issuers' actual cost. The Fed's restriction followed the 2010 Durbin Amendment, which directed the Fed to place limits on debit interchange. Issuers with less than $10 billion in assets are exempt.

The result? The Fed has the option to appeal this latest chapter in the long-running interchange saga to the Supreme Court. For now merchants and their trade groups are celebrating the verdict following years in which they have argued the Fed's limit was excessive. A key part of their argument is that the Fed took account of fixed costs and expenses not specific to the transaction, resulting in a fee cap that was set too high. Merchant groups for years have argued that interchange—the fee they pay for card acceptance—amounts to their largest expense aside from labor.

As some interchange critics have alleged, the fee amounts to "far more than it takes to cover [card issuers'] costs and earn a healthy profit," in the words of Doug Kantor, general counsel for the National Association of Convenience Stores.

But the long-awaited decision may turn out to be an even bigger win for merchants than many realize. Some observers say the ruling is likely to stand up on any appeal, forcing the Fed to impose significantly lower interchange caps. Retail groups have long argued that the Fed's interpretation of the Durbin Amendment has been too favorable to issuer interests.

If that happens, the impact on issuers will be far from subtle. The ruling "will devastate the debit economics of issuing colossi like Bank of America, Chase, and Wells Fargo," warns payments consultant Eric Grover.

Another possible consequence: an advantage for Capital One, which runs its debit cards on the three-party—and Durbin-exempt—Discover network. Potential winners also include PayPal and Block, which work with community banks and so are able to charge higher fees. Durbin only applies to banks with $10 billion or more in assets.

A big mess? You bet.

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

NOVEMBER 2026 • VOL. 23, NO. 8

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

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.

BPA WORLDWIDE

AMEX'S NEXT STEP FOR AGENTIC COMMERCE IS...A FRAMEWORK

There are at least two AI agents available that can make payments on behalf of users, and now payments companies are preparing for a larger role for agentic commerce. American Express Co. in October published a framework for trusted agentic commerce, something it hopes could be part of a larger standard for the payments industry.

The Intent Intelligence Framework is meant to capture and authenticate a customer's purchase intent before an AI agent completes a transaction, AmEx says. What makes this framework unique is that it makes the customer's authorized purchase intent available to issuers earlier in the transaction lifecycle, before the AI agent actually makes the purchase, AmEx says.

The framework complements the issuer's earlier release of a software development kit called Agentic Commerce Experiences. AmEx is chair of the EMVCo agentic commerce working group.

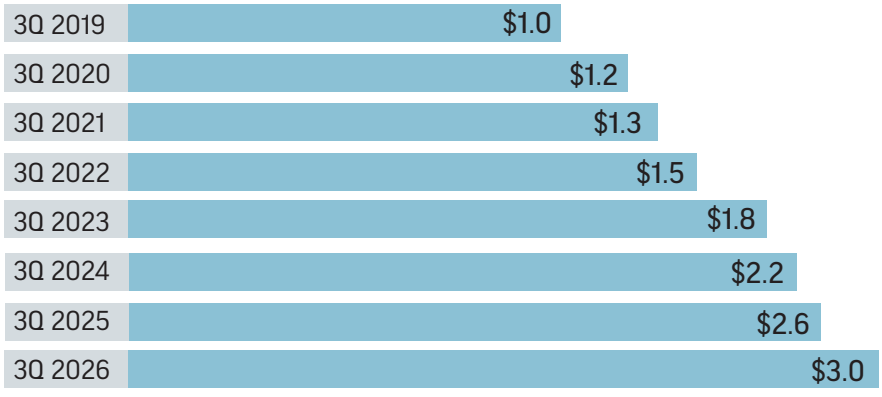
Initially developed with AmEx's business model in mind—it is the issuer, acquirer, and network for its cards—the framework is flexible to work with other models. Its key trait is its flexibility, says Hannah Bozian, AmEx vice president of agentic partnerships.

That's important. Unlike with traditional e-commerce transactions, a new third party, the AI bot, is present when it was just the consumer and the merchant previously. So far, AmEx is seeing "thousands" of weekly agentic-commerce transactions through different integrations the network supports, Bozian says.

"That changes in agentic commerce, Bozian says. "You have a customer, a merchant, and now you've got an agent." In some cases, the customer might tell the agent to find a product and then purchase it. "It's really important to establish what it is the customer is looking for and make sure the merchant is fulfilling what the customer wants," Bozian adds.

WHAT'S IN THE CARDS FOR AMEX

(Net card fees third quarter each year, in billions)



Source: The company

A Platform Built for Partners



Award-winning support that picks up for you and your merchants

> **"I sleep well at night because my clients are taken care of. Support is what keeps merchants for ten years."**
>
> **Mitch Torbett,** Payroc Partner | Watch Mitch's story

When a merchant has a problem, it shouldn't cost you a day in the field. Our support team answers your merchants directly and keeps them processing, so you stay focused on your next deal.

$125B
Annual Volume

190K+
Clients

1,340
Global Operations Team

The team behind every merchant you board

Dedicated partnership team

Onboarding help, deal support, and training on products, pricing, and compliance

Tools and enablement

Pitch decks, product briefs, and training sessions ready when your next meeting is

Operations and risk support

Underwriting guidance, PCI and compliance help, and dedicated risk and fraud teams

Partner with Payroc ›

By sending the customer's intent earlier in the transaction flow, issuers can use that information to make better authorization decisions, she says.

"We think that if issuers have access to this intent data earlier when the customer makes the request and makes their intent known to the agent, we can leverage that," Bozian says. "Whether that is making sure we're making the right authorization decisions, which hopefully results in increased authorizations while also decreasing fraud, agent, and other risks.

"If we have signals that say this might not be what the customer was asking for," Bozian continues, "it might be the wrong merchant, it might be too expensive, it might be the wrong size. And so we think that will help by mitigating those risks, [and it] will drive trust in the overall ecosystem."

Fundamental to the framework is keeping the customer in control of agentic-commerce purchases, she says. "It's not just a capability, it's about keeping the customer in control," she says. "And so knowing that they have signed off on this thing, that they…can edit their intent if they want, they can do that via AmEx or via their agent. And then they can cancel an intent."

The framework has four elements. It starts with the consumer creating and confirming their agentic-commerce purchase intent. The Create Intent API captures these purchase instructions and constraints. Once the customer authenticates their identity, the intent is captured by the agent. The next step is Intent ID, which is a unique identifier created along with a Proof of Intent Token.

This token can be then be used at the time of purchase to obtain a secure digital payment credential that the agent uses at checkout instead of actual credit or debit card data.

In the subsequent phase of the purchase journey, the Intent ID and Proof of Intent Token are used as controls and help validate that the purchase request aligns with what the customer authorized while supporting fraud prevention, authorization decisions, and dispute-resolution measures.

If adopted by other payments entities, the framework would work the same, but would use that issuer's network and tokenization services. "It would depend on their implementation," Bozian says, "but the framework is intended to inform implementation."

—Kevin Woodward

MASTERCARD AND VISA MOVE STABLECOIN SPENDING CLOSER TO THE MAINSTREAM…

Two of the world's largest payments networks announced programs last month geared to bring stablecoins further into the mainstream of money movement. Visa Inc. said its Visa Direct faster-payments platform is launching a commercial service that will incorporate stablecoins.

And Mastercard Inc., with its BVNK unit, has launched its Mastercard Global Money Platform, which brings together the card network's payments technology with BVNK's stablecoin expertise. Mastercard in August closed on its $1.8 billion acquisition of BVNK.

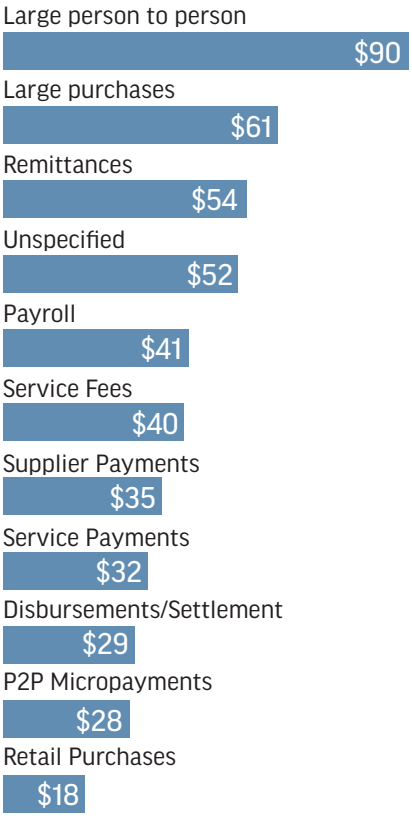
In its latest initiative, Visa has signed up Inyo Global, which the network says has adopted technology needed to offer a commercial service. Based in Cambridge, Mass., Inyo Global offers technology that brings cards, cross-border transfers, and stablecoin capability into a single application programming interface, according to the company.

A connection to Inyo's platform allows businesses to sign up users, accept payments, control fraud, and send domestic and international payouts to more than 180 countries through Visa Direct, according to information from Visa.

Now, the object at Visa is to stimulate stablecoin adoption, particularly for applications such as cross-border transfers, which can

STABLECOIN PAYMENTS BY USE CASE

(Based on spending January through September 2026, in billions)



Source: Allium

be costly on traditional networks. Such international payments are widely seen as a natural first application for stablecoins.

"The next chapter for stablecoins is adoption. Over the last several years, we've worked with several partners and clients to explore how these technologies can improve money movement. We're now seeing those efforts translate into live implementations, helping businesses access more flexible and efficient ways to fund and move money globally through Visa Direct," says Vira Platonova, global head of Visa Direct, in a statement.

Robson Dantas, chief product and technology officer at Inyo Global, says in a statement the venture with Visa will give the company's clients "a new way to fund their payouts, one that is available around the clock." For its part, Visa sees the new venture as a reflection of mounting demand for stablecoin-based processing as a way to manage money movement cross-border at greater speed. Costs for the new service were not immediately available.

For Mastercard, the move to launch the Global Money Platform represents the network's first major integration with BVNK and its stablecoin capabilities. Among the initial users are such companies as Nuvei, Marqeta, Ontop, Beem, and Almond Fintech, the network says. With the platform, users will be able to spend stablecoins at Mastercard-accepting merchants globally. These outlets number in the hundreds of millions, according to the card network.

With stablecoins in place of national and local currencies, users cite what they see as a freer money flow at lower costs. "The future of global commerce depends on money moving as freely as the businesses and consumers it serves, across borders, currencies and increasingly, between traditional and digital forms of money. Stablecoins are becoming an increasingly important part of that future," said Nuvei chairman and chief executive Phil Fayer, in a statement.

—John Stewart

...WHILE MARQETA AND COINBASE WORK ON CARDS BACKED BY STABLECOINS

The card-issuing platform Marqeta said last month it will work with cryptocurrency exchange Coinbase to issue payment cards that businesses can offer to customers, who in turn can use the cards to tap into their stablecoin balances. At least for the time being, the program is aimed at what Marqeta calls "enterprise customers" that use its card-issuing platform.

As with many cryptocurrency-based programs that have emerged so far, the latest venture is geared to simplify the process of spending stablecoins by relying on the familiarity of a payment card. In the background, Coinbase's technology will take care of custody of stablecoin balances and convert digital assets into fiat money. The company's blockchain, Base, will handle settlement, according to Marqeta's announcement. Marqeta will run issuance and payment processing.

Both partners are expecting heightened volume, given the

program's focus on large businesses. "Coinbase brings scale and breadth of infrastructure to provide for the needs of our enterprise customers," says Anthony Peculic, Marqeta's chief strategy officer, in a statement.

The key to this latest venture between Marqeta and Coinbase will be ease of use, observers argue. "On the one side this [collaboration] is fully expected, as technologies like Marqeta try to lessen the friction of a stablecoin purchase," notes Cliff Gray, principal at Gray Consulting Ventures, in an email message. "Because that, after all, is the real battle versus Visa."

"They need me to think it's easier to whip out my Marqueta card than my Visa," Gray adds. "The longstanding challenge at the merchant is the investment required to accept such payment methods. Not always easier said than done."

Some observers see the venture as a move the market might have expected from Oakland, Calif.-based Marqeta. "For Marqueta, this is a way to preserve and enhance their market position, defending it from crypto-native players who may want to sell their own card-issuing platforms. It fills a potential gap in their portfolio," notes Aaron McPherson, principal at AFM Consulting LLC, in an email message.

McPherson also sees expansion possibilities in the program. "I don't think this has to be limited to proprietary cards," he says. "A Visa or Mastercard network affiliation is more likely, and more useful. A proprietary card wouldn't add much value beyond trading the stablecoins directly."

The latest development builds on a prior venture between the companies. Marqeta in 2020 agreed to support the U.S. launch of the Coinbase Card, which was introduced to let users make routine purchases online or in stores. Behind the scenes, Coinbase handled conversion of cryptocurrency into U.S. dollars for both purchases and ATM withdrawals.

—John Stewart

HOW AI'S DEMOCRATIZING BENT IMPACTS FRAUD RATES AND FRAUDSTERS

A new classification of criminal has quickly emerged. Identity-verification and fraud-prevention firm Socure Inc.'s label for this player is the AI-Fluent Fraudster.

In a new report, "From the Frontline: Fraud's Napster Moment," Socure explains why this new classification reflects the burgeoning impact of artificial intelligence. Not only is AI making it easier for organized groups to commit payments and financial fraud, everyday consumers are using it, too.

"On the consumer side, AI has removed the technical barrier to entry," says Mike Cook, Socure's head of fraud insights. "In our survey, 13.4% of respondents said they had used AI to commit at least one type of fraud, and more than half of those AI-fluent fraudsters showed no evidence of committing fraud without it. These aren't career criminals picking up a new tool. They're ordinary people, most commonly men under 30, driven by curiosity as much as by money."

Socure found that 62.7% of AI-Fluent Fraudsters are male compared with 55.1% of those who commit traditional fraud. For its report, Incline Village, Nev.-based Socure gathered data from a survey of 1,253 consumers and information from its global identity and fraud intelligence network.

Many of them are using AI to commit fraud—first-party fraud at 81% is the most common—but others seem to do so out of curiosity.

"Curiosity was their top motivation (41.8%), ahead of economic hardship (37.7%). Fraud has always been driven by need or greed, so curiosity is new," Cook says. "They also feel removed from it: 16.5% said using AI made it feel like they weren't the ones committing fraud, nearly three times the rate of traditional fraudsters (6.1%)."

"First-party fraud has generally been driven by economic hardship and downturns in the economy," Cook adds. "With curiosity taking the lead in motivation, I have concerns that even in a solid

economy, first-party fraud rates may continue to grow at substantial volumes."

These consumers are using AI to create fake hardship letters, fake income or bank statements, skip a BNPL payment, fake a reason for a refund, and avoid paying their credit card bills, the research indicates.

"First-party fraud is the easiest place to start because it can be rationalized as a way to recover money that someone believes they are owed. If the claim succeeds, the consumer learns what the system will accept. The same process can then be repeated across merchants, lenders, gaming platforms, and other industries," the report notes.

Among organized criminals, AI is helping them run their operations more like a business where they can automate attacks and mass produce identities for repeatable profit, Cook says. "Ring members committing first-party [fraud], synthetic identity, or identity theft were far more likely than solo actors to use AI (67.3% vs. 42.9%) and more than twice as likely to work across multiple fraud types."

AI's impact in making it much easier to commit fraud is worrisome. "What worries me is that first-party fraud looks like a gateway to other types of fraud. Synthetic fraud has been flat or slightly down over the past year. It used to be what everyone did. However, that could rise again as people learn they can use AI to build synthetic identities," Cook says.

"That's what makes it more important to look beyond the image. Synthetic documents and deepfake imagery are easy for fraudsters to produce, so it isn't enough to ask whether a document is real. A friend of mine who likes to say, 'If you're solving for a deepfake, you've already lost,' and I think that's right. You have to look at the bigger picture, including device and location data."

—Kevin Woodward

MONTHLY MERCHANT METRIC
Account Attrition %

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.

Date	Account Attrition %	Volume Gross Attrition %	Net Revenue Gross Attrition %
Aug'26 (T3M)	-22.8%	-14.9%	-20.2%

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

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

Account Attrition % - Total attrited accounts in given period divided by total portfolio active accounts from same period of the prior year

Volume Gross Attrition % - Total volume of attrited accounts from given period of prior year divided by total portfolio volume from same period of the prior year

Net Revenue Gross Attrition % - Total net revenue of attrited accounts from given period of prior year divided by total portfolio net revenue from same period of the prior year

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.

THE ONLY MAGAZINE COVERING THE TOTAL PAYMENTS MARKET

In 2022, there were 170.3 billion digital transactions in North America.

Digital Transactions covered them all. It is the only online 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* is your independent source for changes affecting the payments market. *Digital Transactions* is 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.

AGENTIC AI: A NEW PAYMENT SECURITY FRONT

BY GIDEON SAMID
gideon@bitmint.com



AGENTIC AI IS such a powerful productivity boost that even people who are fearful of, and clueless about, AI are embracing it with zeal. The convenience offered by agentic AI, the time saved, is so attractive that even very careful and very reserved people eagerly submit their payment credentials to their personal agent. The agent can buy what they want at the lowest price, delivered when needed, with very little or no intervention on the part of the human user, the agent's owner. By so doing, every agent, aware of the payment credentials of its master, becomes an attractive target for hackers to steal those credentials and run amok, harming the agent's human owner.

The obvious solution is simply to withhold any payment credentials from any AI agent and allow it to do all the work necessary up to the point of pushing the pay button. This is not very practical because some payments need to be executed very quickly, before the attention of the human owner is brought to bear. Some payments are so small that it's ridiculous to summon the attention of the human owner.

The obvious solution, security-wise, is to replace open-ended payment credentials like payment cards with a finite sum of cash. That limits the level of risk and exposure for the user. This is an excellent solution for agents handling small payments, IoT payments, and so on. An agent launched to look for an opportune stock to buy quickly will need to possess the full amount of the purchase price intended by the human owner. Fortunately, digital money today, BitMint for example, is fully ready to serve as limited cash entrusted to agentic AI.

Digital currency carries a cryptographic message that identifies the time, the merchandise or services paid for, the locations, and other information that makes it difficult to cheat.

As we have seen with normal credit card payments, lots of fraud and cheating is occurring without any notice to the human owner. People today are very busy, and when they see a charge of a small sum, they often decide that the time they will have to invest in sorting out this suspicious charge is too costly relative to the value of the charge. In fact, some years ago, a whole criminal industry was based on the idea of milking people through a large number of small, baseless charges.

Payment risk emerges on the other side, too. Institutions that provide various services that are very popular, and tally a large number of customers with payment credentials submitted, themselves become targets for hackers. Many of those institutions are not banks and are not very astute regarding security. The loser is eventually the customer who surrendered his payment credentials.

The agentic AI payment threat is just a small part of the overall threat presented by AI. One may argue the industry is going in the wrong direction. Under the guidance of the National Institute of Standards and Technology, banks and financial institutions are building greater complexity to fend off attacks from quantum computing and AI. But that complexity is eventually vulnerable. It surrenders to a smarter-than-expected mathematician.

The right direction is to use "cyber oil," the equivalent of the crude oil of the 20th century. Cyber oil is randomness. The more randomness you put into your security, the more secure you are. AI and quantum cannot defeat randomness. A lot of financial catastrophes will have to unfold before this simple fix happens—before the community realizes that "pattern" means "vulnerability" and "randomness" means "security." DT

INTERCHANGE, CHARTER PARITY, AND THE FDIC



BY BEN JACKSON
bjackson@pa.org

AN ATTEMPT TO limit the interchange merchants pay in Illinois has started a larger conversation about the power of various financial-institution charters.

In 2024, the Illinois legislature passed the Interchange Fee Prohibition Act, which would have excluded taxes and tips from the calculation of interchange merchants pay for card transactions. Originally scheduled to go into effect July 1, 2025, the law's effective date has been pushed out twice and now is July 1, 2027.

But the implementation may not come at all for national banks and institutions chartered outside of Illinois.

In April, the Office of the Comptroller of the Currency issued an interim final order that federal chartered banks were exempt from the Illinois Interchange Fee Prohibition Act because the National Bank Act and the Home Owner's Loan Act preempt state laws.

Additionally, this year a judge from the Northern District of Illinois entered an injunction against the act for national banks, federal savings and loans, and out-of-state chartered banks. Judge Virginia Kendall expanded that injunction in September to include national credit unions.

To further protect state-charted banks, the Federal Deposit Insurance Corporation published a rule in the Federal Register in September that would prevent the laws of one state from applying to banks chartered by another state. Currently, the FDI Act offers pre-emption of state laws for banks chartered by a different state, but the law was written in the context of interstate branches. So, it has been interpreted to offer pre-emption only to out-of-state banks that have established a physical presence in another state.

The rule would expand that pre-emption so that it applies even if the out-of-state bank has no physical presence in a host state.

The proposed rule has raised a quiet debate inside the industry over whether state-chartered banks should have the same pre-emption as national banks. Some national-bank charter holders have concerns that the FDIC rule would dilute the value of a national charter, while others say that this is just an extension of the current state of affairs.

At the same time, the Conference of State Bank Supervisors has come out in support of the parity rule. While state regulators want to be able to supervise the banks chartered in their states, the regulators from state A do not want banks with a charter from state A to have to comply with the rules of state B. That would dilute the value of their charters.

Of course, another danger of letting each state law stand is that, if every state passes individual laws on topics like interchange, payments providers could suddenly find themselves having to manage up to 50 different compliance regimes. This would create confusion for cardholders, merchants, and payments providers.

Merchants, especially those near transportation hubs, would have a harder time evaluating payments costs than they do now as they try to sort out what they would owe for transactions made with out-of-state versus in-state cards, for example. Payments providers would need to create systems that could manage all the different states and figure out how to manage the costs and settlements for each transaction. Cardholders might find some forms of payments discouraged or not accepted.

On top of all of this, the rules would only apply to payment card transactions. This might prompt merchants to encourage payment forms such as cash, pay-by-bank, person-to-person transfers, and stablecoins. It could shift the balance of payments away from cards.

The comment period on the FDIC proposal closes Nov. 23, so there is still time to weigh in on the proposed rule and encourage a level playing field for financial institutions of all charters. DT

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

WHEN SOMETHING ELSE SPENDS YOUR MONEY

Governance and risk management will be necessary in the agentic era, and will likely be tested in novel, challenging—and unpredictable—ways.

BY **CLIFF GRAY**

Cliff Gray is Founder at Lakeland Scientific, a payments analytics and consulting firm.

AT ITS CORE, agentic commerce is a natural outgrowth of the greater AI phenomenon. Industry and individuals alike have been using AI agents to perform tasks of all kinds. Letting those agents buy things was a foregone conclusion from early on. AI can develop working Web sites in moments, architect mobile apps, solve age-old medical mysteries, and seemingly answer any question we can formulate. Surely buying things would be child's play for artificial intelligence.



Photo: 123RF/pitinan

The payments industry has embraced the phenomenon, welcoming the potential boost to purchasing volume. Visa and Mastercard, perceiving agentic commerce as in perfect tune with their greater philosophy of reducing friction for the consumer, have each defined protocols and methods to identify and validate these transactions separately from other payment channels. The networks were quick to recognize the challenges inherent in agentic commerce, as much as they saw the potential business opportunity.

What they and the greater industry recognized was the fundamental originality of the agentic phenomenon: something, not someone, would have the authority to make a purchase based on the cardholder's specifications and using the cardholder's funds.

Everyone is familiar with the potential pitfalls of someone else spending your money. Yet in many scenarios, this is a normal course of doing business. Delegated spending is commercially routine as commerce already knows how to keep delegated financial authority within acceptable risk boundaries. This reliable commerce framework must shape, in some way, how

agentic commerce evolves into its own reliable commercial framework.

GOVERNANCE IS KEY

The greater challenge, then, may not be engineering, but administration. Agentic commerce introduces an extraordinarily consequential abstraction into payments, and that requires incredibly effective governance, authority, and control. Software is no longer merely facilitating a consumer's purchase. It may be authorized to decide what to purchase, from whom, when, and for how much. This distinction should not be underestimated: it's about something, not someone.

Payments architecture has spent decades establishing increasingly sophisticated methods to authenticate consumers, protect credentials, detect fraud, assign liability, resolve disputes, and provide an auditable chain of events. Agentic commerce now inserts an autonomous decisionmaker directly into that carefully engineered framework. Somewhere, Pandora is grinning knowingly.

What constitutes consumer authorization when an agent makes a purchase the consumer did not specifically approve? Who bears responsibility when an agent misunderstands instructions, selects the wrong merchant, exceeds an intended spending threshold, or simply makes a bad decision? The issuer? The merchant? The consumer? And how does a merchant distinguish a legitimate autonomous purchase from compromised software behaving exactly as it was designed to behave?

Artificial intelligence and branded payments. Arguably, here is the marriage of a purposeful liar to a purposeful spender. It is a known fact that AI, by its own nature, hallucinates. In that light, the previous maxim takes on a frightening new perspective. Software is no longer merely facilitating a consumer's purchase. Instead, it may be hallucinating a consumer's purchase.

As humans, we don't consider this type of problem. It's a perspective we cannot have. I don't worry that my chief financial officer will suddenly and inexplicably invest 90% of the company's capital in space monkeys. Not just because my CFO is not prone to hallucinate, but because I trust that he knows better without my needing to explicitly exclude such an investment. That's one tricky thing about AI agents—it's going to prove difficult to tell them all the things not to do.

Many of these challenges are being addressed already, in one form or another. Today, agentic transactions remain fundamentally card-not-present transactions, with chargebacks governed by the existing frameworks for tokenization and dispute resolution. Policies around chargeback liability are firmly putting the onus on the cardholder. It's your agent, your purchase, your liability. As downstream issuers embrace the new protocols defined by the card networks for agentic authentication, these new authorization models will ultimately influence how agentic transactions are classified, priced, and assigned liability.

Related to the unprecedented nature of AI itself, the authentication models being finalized currently are a rare departure from the long-time standards of ISO 8583 and ISO 20022, which represent the backbone of branded payment systems today.

Issuers and other interested parties will have to look outside these normal channels for the data necessary to properly authenticate agentic purchases in real time. Just as important, issuers must rely on these new data channels to reliably tie their cardholder to the agent making the purchase. This could prove challenging for smaller issuing institutions and their technology providers.


Gray

Gray: "Before we teach software how to spend our money, we should be extraordinarily certain we have taught the payment ecosystem how to constrain it, authenticate it, audit it, and stop it."

There is a certain irony in racing toward autonomous commerce while the United States still embosses yesterday's vulnerability onto the back of tomorrow's payment card. Before entrusting software agents with independent purchasing authority, perhaps we should finish retiring the magnetic stripe, a technology whose expiration date preceded the intelligence now being asked to use it.

THE DISPUTE CHALLENGE

The branded payments industry relies on dispute and chargeback handling. Until network and authentication protocols evolve accordingly, dispute resolution for agentic commerce will remain little better than the remediation process it is today for e-commerce and card-not-present transactions: identify the problem, then claw the money back after the fact.

Agentic commerce introduces delegated purchasing authority. It therefore demands controls capable of validating, constraining, and, when necessary, stopping that authority in real time, just as conventional fraud-prevention systems work today around conventional cardholder purchasing models. Legacy dispute resolution, by contrast, is a recovery mechanism that cannot support a problem exacerbated by the speed of AI. Agentic commerce will increasingly demand prevention before authorization.

Across the payments universe, policies and procedures have been hardened, broken, updated, hardened again, and so on, over decades. They respond to new technology threats, new actor threats, new technologies to defend. Now, the advent of agentic commerce will force a rethinking of these sophisticated fraud-control structures in a fundamental way. The payments industry is facing behavioral changes of unknown size and shape.

An effective purchasing agent may deliberately go where its owner wouldn't, shopping at unfamiliar merchants, purchasing unusual products, or transacting at unusual times. These are precisely the behaviors conventional fraud systems have been trained to distrust: an artificially intelligent agent, bound and determined to please its master, with no reliable failsafe for giving up, and tirelessly seeking any means necessary to find that widget. Your Visa card in its virtual hand. A hand belonging to something, not someone.

Today, real intelligence around agentic commerce remains at the merchant edge, but is moving towards normalization within the networks and their issuing partners, so agentic commerce can be treated as such in real time. Visa and Mastercard have built out the fundamentals and are finalizing policies so the greater payments ecosystem can reform to support agentic commerce. How fast payment ecosystems react, and how successfully, remains to be seen.

A fundamental, yet unspoken, shift that agentic commerce presents concerns convenience, ever the theme for Visa and Mastercard as they seek to lure more consumer activity. Merchants, acquirers, networks, and issuers are all striving to remove friction for the consumer, which goes a long way towards making the sale. To date, trusted architectures have always preceded buyer convenience. Agentic commerce reverses that priority, assuming the architecture will overcome the risk. Pandora is grinning again.

Before we teach software how to spend our money, we should be extraordinarily certain we have taught the payment ecosystem how to constrain it, authenticate it, audit it, and stop it.

SIMPLER, SAFER

In the end, all my years of payment experience may have little to do with my final thoughts on agentic commerce. It was my experience as a parent that provided the compromise. When your petulant 14-year old who thinks he knows everything needs some purchasing power, you give him a prepaid Visa with a couple hundred bucks on it, not your Black AmEx accepted at the local Mercedes dealership.

Until the payments ecosystem develops comparable boundaries on agentic commerce, that seems a simpler, safer way to stop something from buying something it shouldn't. DT

THE ONLY MAGAZINE COVERING THE TOTAL PAYMENTS MARKET
Subscribe today!
Visit Bolandhillmedia.com/dtr to start tackling the ever-changing payments market.

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

Merrick Bank

© 2026 Merrick Bank. All Rights Reserved.
The stylized M design is a trademark of Merrick Bank.



50 WAYS TO LEAVE MAGSTRIPE

General purpose cards long ago moved to chip. Now, EBT/SNAP cards are doing so, but in 50 different ways.

BY KEVIN WOODWARD

In the 21 months since California began rolling out chip versions of its electronic benefits transfer cards, used with the Supplemental Nutrition Assistance Program and other assistance, it has reduced the theft of food and cash benefits by 83%.

When announced in January, the fraud rate—no updates have been issued since then—fell from more than $20 million in losses in January 2024 to approximately $4 million by November 2025.

California was the first state to begin its EBT/SNAP card migration to chip. The adoption of chip and PIN technology—no chip and signature for these cards—was one part of the state's effort, along with forcing PIN resets and law enforcement coordination, that helped drive down the fraud rate. California has the most SNAP recipients, with an estimated 5.47 million monthly SNAP recipients, according to USAFacts.org.

More than 11 years since general purpose credit and debit cards adopted chip technology to better secure card transactions, EBT cards are just getting going. Why has that taken so long? What does the rollout mean for acquirers, independent sales organizations, and merchants?

The short answer is 50. Each state administers its own benefits program and each state is at different stages and follows unique directives from its elected leadership. Currently, just eight states, including California, are issuing chip-based EBT cards, according to the U.S. Department of Agriculture, which administers the program at the federal level. The others are Oklahoma, Alabama, Virginia, Maryland, New Jersey, Massachusetts, and Michigan. Another six—Oregon, New Mexico, Arkansas, Pennsylvania, New York, and Maine—have EBT chip card projects in progress.

The USDA also says SNAP retailers in 26 other states, in addition to the 14 above, must be prepared to accept out-of-state EBT chips at their locations. The remaining 10 states have no announced conversions. The agency also intends to test a mobile wallet version of delivery SNAP benefits, with a pilot scheduled in Illinois in 2027.

The USDA Steps In

Many states, over the years, may have anticipated federal legislation that would provide overall direction, but that had not materialized, says Anna Sever, president of Conduent Inc.'s government solutions unit, leaving many states on their own. That's 50 different timelines, 50 different ways of providing the same service.

"We waited to see if the federal legislation was passed," Sever says. "Federal legislation did not get passed. So states then said, we're going to do it ourselves." Florham Park, N.J.-based Conduent and Jacksonville, Fla.-based FIS Inc. dominate among core state EBT host processors.

That is, until late October 2026, when the USDA issued a proposed rule that all states would have to adopt chip-enabled EBT cards that also have NFC technology to enable contactless payments. Written comments on the rule are to be accepted through Dec. 22. It is unknown if or when the rule might be approved, but the proposed rule suggests a two-year timeframe from the publication date of the final rule. Comments are sought, too, on whether that is sufficient time for compliance and to counter EBT fraud.

The EBT/SNAP program went through a similar conversion when states migrated from paper coupons—a.k.a. food stamps—to card-based delivery of funds. It's not surprising to Prashant Gupta, general manager of government solutions at FIS.

Photo: 123RF/liudmilachernetska

FIS converted its first program from paper to card in 1991. That conversion for the entire industry took almost 20 years, he says. "And actually, we just converted the last territory two years ago, Commonwealth of the Northern Mariana Islands," Gupta says.

Most U.S. territories, such as the Northern Mariana Islands, participate in a similar assistance program, but not SNAP. EBT chip cards use the same EMV technology as on general purpose chip-enabled credit and debit cards, albeit with specialized applications for their unique payment needs.

50 Priorities, 50 Budgets

Another reason the migration to chip for EBT cards is taking a while is that each state has its own priorities and budgets.

"Every state has their own procurement statutes, laws, guidelines, guiding when to procure these services," Gupta says. "Some states procure for three years, some states procure for seven years, some procure for seven plus years. So it's just different cycles of procurement."

Each state's population is a factor, too, Sever says. "You have some states with multiple very large population centers, like California. You have some states with maybe one large population center," she says.

In addition to California, Massachusetts, Maryland, and Michigan are debuting their EBT chip cards this year, Gupta says. New York, New Mexico, and Oregon are expected to do so in 2027, he says. Alabama began issuing chip versions of its benefit cards in December 2025 with a statewide rollout in February.

Once state legislators give the OK to migrate to chip for their benefits programs, the work begins in earnest to prepare merchants and recipients for the cards.

In some cases, merchants may have to replace their point-of-sale terminals even though they are EMV compliant, says Gupta. In some cases, he says, that's because they're old or may not be able to accept software updates, with the latter seen more often.

"But the whole challenge was that every retailer had to make sure that their terminal is compatible for taking those transactions, right?" he says. The situation has improved a lot. FIS sees 40% to 60% of EBT transactions on its networks processed as dipped or tap transactions, says Gupta. California's card, called the Golden State Advantage, also is contactless enabled.

Convenience stores often need new EBT chip-compliant terminals, Sever says. To get these POS devices installed, Conduent uses an array of methods, from sending devices directly to merchants to using a third-party distributor to ship terminals.

There can be delay getting terminals updated if the state government and its retailer associations lack a uniform message about the need for them, Sever says.

Using Conduent's Alabama contract as an example, Sever says state administrators and their interaction with retailers can aid the transition, as it did in Alabama. Approximately 740,000 individuals receive SNAP benefits in Alabama, according to USAFacts.org.

"It's when the states aren't that clear with their retailer associations that the rollout becomes delayed and delayed and delayed," Sever says.



Gupta: "Every state has their own procurement statutes, laws, guidelines, guiding when to procure these services."

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.

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

www.gcfinc.com • (888) GCF-NEWS



Sever: "It's when the states aren't that clear with their retailer associations that the rollout becomes delayed and delayed and delayed."

Gupta also says the retailer messaging is essential. In the case of California's migration, that meant getting retailers ready and engaging with associations within the state and outside of it, he says.

Diversity in Fraud

Educating recipients also was crucial. Instead of simply swiping the magstripe on the back of the earlier cards through a terminal, they needed to know the chip version must be dipped into a slot and left there until after inputting a PIN and waiting for the safe-to-remove signal.

That's not all cardholders will notice. Many states, such as California, are making their EBT cards dual interface, allowing users to tap to pay for their purchases. Cardholders also can make online food purchases with the SNAP program, hence the online PIN requirement. DoorDash Inc., a third-party delivery company, enabled online SNAP/EBT payments for Dollar General in 2025 and Walgreens Co. enabled online SNAP acceptance via Instacart, another delivery firm, in 2024.

Of course, one of the primary motivators for all this change is to help reduce fraud. California is the only state to have released data on EBT fraud rates affected by chip card use.

In addition to recipient and retailer fraud, EBT benefits also are targeted by criminal rings, Sever says. These attacks made by organized criminal rings mostly originate overseas, she says. EBT participants might fall victim to phishing attacks. Sever says they are not unlike criminal rings that target elderly Social Security recipients.

These diverse fraud vectors mean agencies and vendors must embrace multiple fraud prevention measures, Gupta says. "Fraud happens in so many different ways in EBT, and we basically look at this from all different angles," he says. "We are bringing different technology solutions into this market."

For example, FIS provides a mobile app that enables EBT users to lock and unlock their cards, just as many general purpose issuers do for their cardholders. Conduent offers the same service. Some states, such as Alabama, also automatically block out-of-state transactions.

'Smart Decisions'

With more states preparing to adopt chip cards for the EBT programs, the outlook is fairly promising, though, as the EBT sector has proven, it may not be a quick process.

Gupta suggests California's fraud reduction results may prompt more states to consider new cards. Because of that impact, an 83% reduction, he hopes it can spur more activity. The pending mobile wallet pilot next year may also spur interest.

Sever says the market for EBT contracts is competitive and any ability by a vendor to ease chip conversion could be a selling point as states enter the procurement stage.

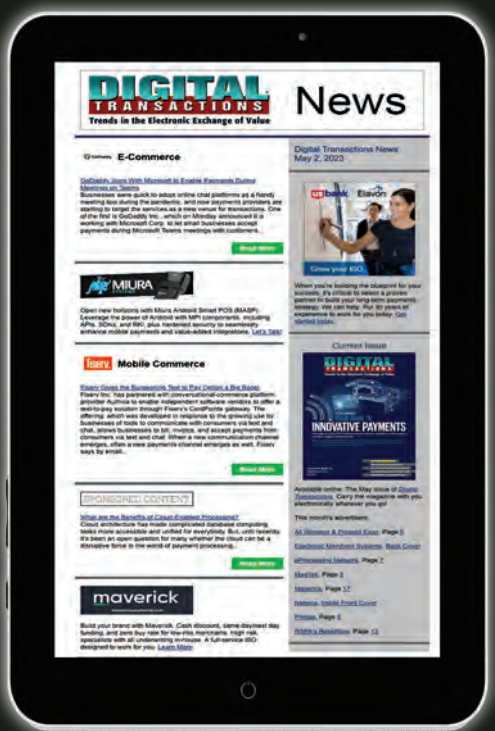
While chip cards and POS terminal updates have critical roles, the real effort is not technology alone, but when updates are made in conjunction with education.

"It's a combination of using the technology and then helping folks make smart decisions about how they use their card and transact on their card. That's the only way we're going to be able to fight fraud if we do it on both fronts," Sever says. DT



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**

STRATEGIES FOR REVENUE PROTECTION, PART II

Last month, we looked at payments lost to fare evasion in mass transit. Now, it's time to examine the threat of fare fraud and how to confront it.

BY **AUDREY DENIS**
Audrey Denis is director of new ventures, Cubic Transportation Systems.

AS WE DISCUSSED last month in Part One of the *Strategies for Revenue Protection* series, transit agencies are facing mounting financial pressures, and the need to protect every dollar of revenue has never been greater.

Fare evasion is a well-known threat to revenue and has visible indicators, like gate jumping. But fraud is a different threat vector to revenue entirely. It is often enabled by technology, and exploits system loopholes like first-ride risk abuse or short ticketing. It also requires an entirely different set of tools and strategies to combat.

To protect revenue, it's critical to understand the distinction between fare evasion and fraud so agencies can adopt tailored strategies to address these evolving threats.

If transit agencies want to stay ahead of fare fraud, innovative solutions are a must. In this article, we will explore the various methods of fare fraud, how agencies can begin enacting changes to combat it, and why it is imperative to start working toward fraud reduction now.



Photo: 123RF/grispb

MODERN FARE FRAUD

A common misunderstanding when it comes to fare fraud is that it's just fare evasion in disguise. This could not be further from the truth. Fare fraud is a separate, often more complex challenge.

Part of what makes fare fraud so challenging is that many fraud strategies are often invisible to enforcement officials and can be difficult to identify due to loopholes within the ride system itself.

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.

Common fraud vectors include:

- **First Ride Risk Abuse:** Riders exploit the delay between gate access and account validation by using newly provisioned cards with no funds. They ride free before the system can deny the transaction.
- **Card Re-Provisioning:** Fraudsters remove and re-add prepaid cards to mobile wallets, resetting the system's recognition and bypassing blacklists.
- **Short Ticketing:** Particularly prevalent in distance-based fare models (as in the U.K.), riders purchase multiple short-distance tickets to pay for incomplete segments of the full trip.

The complexity of these tactics, and their ability to evade detection through traditional means, underlines the need for agencies to move beyond traditional fare enforcement and embrace technology-driven solutions.

TECHNOLOGY'S ROLE

The fare fraud tactics mentioned above exemplify how fraud is not just a behavioral issue, it's a technical one.

That is why technology plays a pivotal role in closing fraud loopholes. As fare fraud evolves, transit agencies must rely on advanced systems that not only support seamless rider experiences but also actively detect and prevent abuse.

Modern fare-payment system providers are leading this charge with innovations designed to close loopholes and protect revenue in real time. These include:

- **Real-time Account Validation:** Transactions are checked instantly. If a credential is in bad standing, it's immediately declined, or if it lacks funds, it is added to a deny-list. Additionally, calculating fares in real-time and keeping a live picture of operations and riders helps minimize the window for fraud caused by lag and offline checks, resulting in a reduction of short-ticketing fraud and prevention of refund requests for journeys that have already been taken.
- **Primary Account Reference (PAR) Matching:** This links multiple credentials tied to the same funding source, preventing re-provisioned cards from entering the system if they have associated debt and enabling debt recovery across associated credential types.

As fraud schemes expand, it's important for agencies, fare-payment vendors, and card schemes to actively collaborate to close known loopholes and position themselves as advocates for transit agencies.

Technology is a key factor in combating fare fraud. But it must do more than support fare collection if we hope to combat fare fraud at the rate at which this crime is evolving. Agencies need to identify their pain point with fraud and equip technologies that empower them to enforce policy, protect revenue, and act proactively.

AI AND MACHINE LEARNING

Fare fraud is only going to become more sophisticated as time goes on. If transit agencies want to keep up, they will need equally advanced tools at their disposal to detect and respond to it.

Artificial intelligence (AI) and machine learning (ML) are transforming how agencies understand and combat fraud. An example of this can be seen through the research being conducted by Cubic Transportation Systems and Imperial College London that is driving innovation in fraud detection. Through these research efforts, agencies are able to develop



Denis: "While fare fraud may be harder to see than fare evasion, its impact on revenue can be just as severe."

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

models that analyze rider behavior and identify patterns of fraud, such as short ticketing.

For instance, as stated in their "Short Ticketing Detection Framework Analysis Report," we now know that there are five distinct short-ticketing types:

- **Ghost Station** – Stations where passengers only enter or exit, but never complete full journeys. These stations may be used as decoys or bypass points and are not functioning as part of legitimate journeys.
- **Black-Hole Station** – There are disproportionate exit-only ticket patterns at these stations, suggesting explotation as unauthorized exit points.
- **Fake-Origin** – Passengers may be using these stations to simulate a legitimate journey start, while actually boarding elsewhere.
- **Function-Loss** - Extreme declared destination/declared origin ratios at these stations indicate a breadown in normal usage.
- **Micro-Trap behaviors** – Subtle anomalies shown in these low-volume stations are harder to detect but may signal emerging hotspots for exploitation.

Each of these patterns represents different exploitation mechanisms for fraud, enabling a specific operation possibility. Models can help agencies precisely identify the stations where fraud is occurring, how fare policies may inadvertently encourage abuse, and which payment methods are being exploited.

By implementing the developed short-ticketing detection algorithm, agencies can now precisely deploy revenue protection staff to stop passengers attempting to travel with short ticketing. This approach provides more targeted patrols, allowing for the optimization of human resources.

Ultimately, AI and machine learning are not just tools for detection. They are engines for smarter decision-making. By integrating these technologies, agencies can move from reactive enforcement to proactive revenue protection, ensuring that every dollar is accounted for and every loophole is addressed.

COLLABORATION IS CRUCIAL

As fare fraud continues to become more complex, the need is clear for collaboration to combat it. Protecting transit revenue is not the sole responsibility of any one entity. It is a shared effort that requires coordination across agencies, technology providers, and payment networks.

Transit agencies play a foundational role in combating fare fraud by designing smart, equitable fare policies. These policies must balance accessibility with enforcement, ensuring that riders who qualify for reduced fares can easily access them, while also discouraging opportunistic or habitual fare evasion.

Technology vendors are responsible for providing the tools that make these strategies effective. Their platforms are not only responsible for supporting fare capping and reducing fare eligibility, they must also offer real-time fraud detection, denylist management, and AI-powered analytics. These tools help agencies enforce policy, close loopholes, and recover lost revenue.

Payment networks and card schemes also play a critical role. Many fraud vectors exploit vulnerabilities in how mobile wallets and payment credentials are managed. The collaborative approach outlined here allows fraud to be a shared responsibility, and that, in turn, results in accelerated innovation, quick action, and improved outcomes across the board.

FINAL THOUGHTS

While fare fraud may be harder to see than fare evasion, its impact on revenue can be just as severe. Combating it requires a multipronged approach: real-time data, policy alignment, and collaborative innovation.

With the right technology and partnerships, agencies can stay one step ahead of fraudsters and safeguard the revenue they depend on to serve their communities. DT

ADVERTISER INDEX

Digital Transactions Pages 8, 11, 21, 23, IBC, BC

General Credit Forms, Inc. Page 19

Global Payments Inside Front Cover

Merrick Bank Page 15

PayRoc Page 4

FRAGMENTED TECH IS RESHAPING AI ECONOMICS

In business, getting AI right is critical. In restaurants, the stakes have never been higher.

BY MANUEL SCHOENFELD
Manuel Schoenfeld is chief strategy officer & chief AI officer at Qu.



Photo: 123RF/creativestocks

PAYMENTS TECHNOLOGY learned a critical lesson decades ago: Commerce cannot and will not stop when connectivity issues arise. Store-and-forward and other resilient strategies allowed transactions to move locally and synchronize centrally when connectivity returned.

Now, as restaurants apply AI to their drive-throughs, kitchen workflows, inventory, and other time-sensitive functions, the same lesson is still essential. Not every decision needs to travel to the cloud and back.

This lesson is both economically and operationally important. Cloud AI pricing typically depends on usage, including tokens, requests, compute time, or data transfers. A single request may cost very little, but restaurant operations generate massive transaction and decision volumes across ordering, payments, kitchen and back-office systems.

With every API call, inference, or data transfer, the digital meter rises. When multiplied across several locations, these unaccounted-for costs erode already thin restaurant margins. Now, take this same approach across dozens or hundreds of locations, and those requests quickly become an operating expense rather than a one-time technology investment.

Reliability and fragmented data add to the list of challenges when scaling cloud-only AI. The Amazon Web Services outage in 2025 showed how dependent digital operations can become on centralized infrastructure. A hybrid edge-cloud model addresses these challenges by processing immediate workloads locally while leveraging the cloud for critical centralized analytics, reporting, and cross-location intelligence.

UNIFIED DATA IS FOUNDATIONAL

Even with advanced AI models, the quality and unification of data remain critical to effective implementation. Traditionally, operators have adopted one solution at a time, often deploying separate platforms for point-of-sale, payments, kitchen management, and drive-thru operations. In this deeply fragmented environment, information is siloed, forcing each system to generate its own version of the same data and creating inconsistencies that can undermine AI effectiveness.

Even the most advanced AI models struggle to produce actionable insights when fed inaccurate or incomplete data. When payments, POS, kitchen, labor, and loyalty systems are connected through an intelligent commerce platform, high-quality data can give operators a better perspective on performance, generate deeper insights, and protect already thin margins.

AI investment should not be treated as an all-or-nothing decision. These investments must be made intentionally and strategically. Prioritizing data unification first, then deploying hybrid edge-cloud architectures, establishes the foundation for AI to deliver meaningful returns. From there, operators can confidently determine which workloads belong in the cloud and which should be processed locally.

HYBRID EDGE-CLOUD MODELS

The case for hybrid deployment is becoming concrete. According to the NRA's "2026 State of the Restaurant Industry" report, 26% of restaurant operators are already using AI-assisted tools. But adoption is concentrated in relatively limited use cases.

According to the report, marketing leads adoption, followed by AI-assisted administrative tasks, and finally, customer orders. As AI usage expands into higher-volume operational workflows, the architecture decisions that operators make today will determine whether future deployments remain affordable at scale.

Typical AI pricing is measured by usage, including tokens, requests, compute time, or data transfer, and costs vary by model and workload. A restaurant using AI for 10,000 small operational decisions per store each day would generate 300,000 cloud-supported decisions per month from a single location.

Across 10 locations, that becomes 3 million monthly decisions before accounting for prompt changes, peak-period spikes, integrations or model upgrades. In an industry that often works within 3% to 5% pre-tax margins, any recurring infrastructure costs can become meaningful if routine decisions are routed through the cloud.

Hybrid edge-cloud models empower restaurants to process routine, time-sensitive decisions inside the store while still using the cloud for broader analytics, reporting, and cross-location strategy. Stores will still run AI models but will do so locally instead of relying solely on the cloud.

The benefits of processing at the edge include:

- **Stable Connectivity:** Regardless of Internet or service connectivity status, edge-enabled devices ensure decisions about order sequencing, kitchen workflow, and predictive staffing happen instantly. This stability fosters a system that is both cost-efficient and resilient.

- **Autonomy:** Restaurant operations are inherently unpredictable, from breakfast rushes to dinner peaks. Edge computing gives store teams a certain level of autonomy by computing locally. This allows teams to focus on revenue-driving operations instead of waiting for feedback from centralized systems. And the enhanced autonomy gives managers immediate control over operations.

Enhanced guest satisfaction: 57% of surveyed restaurant brands ranked digital guest experience a top investment area for 2026. Yet the biggest barriers include operational execution, fragmented systems, and staff retention. Edge-enabled AI can bridge that gap by processing decisions closer to the restaurant, supporting faster, more accurate service.

Integrating edge and cloud computing does not mean abandoning centralized oversight. Historical analytics, cross-location comparisons, and strategic forecasting can all be saved in the cloud, while local intelligence handles workloads where speed, resilience, and transaction volume matter most. Together, the two environments allow restaurants to match computing resources to the economic and operational requirements of each use case.

The pressure to protect margins while adopting AI — not simply to innovate, but to remain competitive — has never been higher. Increased labor and food costs are driving demand for intelligent automation, but operators cannot afford to layer another disconnected system onto an already fragmented stack.

Operators that successfully deploy AI with careful attention to both infrastructure and data quality will be the ones with a competitive advantage. DT

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.



The payments market is large and fragmented.

DigitalTransactions.net gathers the most important news in one place, and shows you how it all fits together to impact your business.



Concise, clean interface is easy to navigate

Breaking news from the payments market, posted daily

Calendar of industry events

Complete current and past issues of *Digital Transactions* magazine

Detailed listings of payments market suppliers

13 years of payments news and analysis

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value