DIGITAL TRANSACTIONS®

Trends in the Electronic Exchange of Value

AGENTS OF RISK

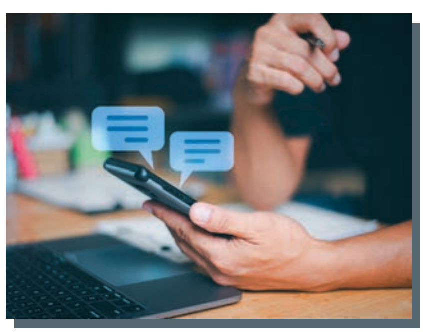
Artificial intelligence has had a year to gestate. Now, as the critical fourth quarter beckons, both good and bad uses of AI are ready to take control of the checkout.

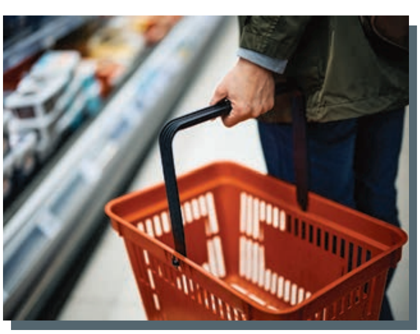
Volume Twenty-two, Number Nine • DigitalTransactions.net • September 2025

ALSO IN THIS ISSUE:

contents

SEPTEMBER 2025 • VOLUME 22, NUMBER 9





Cover: 123RF/Generated by AI

Digital Transactions (USPS 024-247) is published monthly by Boland Hill Media LLC, 800 Roosevelt Road, Building B, Suite 212, Glen Ellyn, IL, 60137. Periodicals Postage Paid at Glen Ellyn, IL, and at additional mailing offices. POSTMASTER: Send address changes to Digital Transactions, P.O. Box 493, Northbrook, IL 60065-3553.

the gimlet eye

CAN PROCESSORS HELP CUT MERCHANT COSTS?

WITH MERCHANTS GROWING more heated in their opposition to card-acceptance costs, processors are looking for strategies that could help sellers gain from improvements in card authorizations. An important example of this emerged this summer with news from the big Canadian processor Nuvei Corp. It launched a pair of technologies it says could boost card-authorization rates for North American merchants by as much as 3.5 percentage points. Will that claim hold up? We shall see.

The two services, PINless debit and least-cost routing, are far from novel, but they could help merchants "bypass traditional card rails in favor of lower-cost debit networks," says Nuvei, which is making the services available now in the U.S market. "These enhancements give merchants access to debit networks that can deliver both higher approval rates and lower processing costs," claimed Philip Fayer, Nuvei's chairman and chief executive, in a statement.

The company, which deploys what it calls a "smart routing engine" that depends on artificial intelligence and machine learning, says it looks to route transactions "through the best-performing banks or card network." For debit cards, the system looks to send transactions through what the company calls "lower-cost" networks, though resort to Visa and Mastercard is available if needed.

A bit of background: Debit cards account for more than 53% of online card volume in North America, Nuvei says. Regulation in the U.S. market in recent years has aimed at enhancing merchant choice in network selection, with the aim of introducing more competition. One such regulation, the Durbin Amendment, applies to debit cards and became law in 2010. Similar legislation for credit cards, the Credit Card Competition Act, is under consideration in Congress and would require that processors offer merchants a choice of networks beyond Mastercard or Visa.

Debit networks, too, have been seen by some experts as entities that could play a larger role in handling credit card transactions, though network officials typically avoid comment on this hot-potato subject.

Experts also point to companies not often seen as direct competitors to Visa and Mastercard as alternatives that could offer enough competition to reduce merchant costs. They often point to Venmo, a peer-to-peer payments network owned by PayPal. RTP, or the Real Time Payments network, is another candidate cited by some. It's part of The Clearing House Payments Co., a system owned by some of the nation's largest banks.

While most proposals depend on network competition to cut transaction costs, Nuvei could be offering a novel approach by focusing on acceptance rates. But merchant savings from Nuvei's initiative is difficult to project, experts have told *Digital Transactions*. Time will tell, but this is a welcome alternative to legislation and litigation.

John Stewart, Editor | john@digitaltransactions.net

SEPTEMBER 2025 • VOL. 22, NO. 9

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

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.

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.

trends & tactics

SORTING WINNERS FROM LOSERS IN DEBIT

With merchants prevailing in their long-running legal battle to overturn debit rate caps set by the Federal Reserve, the largest debit card issuers could wind up the biggest losers, while Capital One Financial Corp. emerges as the big winner.

U.S. District Court for the District of North Dakota Judge Daniel M. Traynor in August delivered a huge blow to debit-issuer revenues with a ruling that the debit card interchange rates set by the Fed must reflect issuers' actual cost per transaction. The Fed can set set debit rate caps under the under the terms of the Durbin Amendment to the Dodd-Frank Act, enacted 15 years ago.

Prior to Traynor's ruling, the Fed set debit caps using a so-called blended formula that takes into account myriad costs issuers incur with a debit card transaction, including fraud prevention and fraud loss recovery. Tying debit rate caps more closely to actual per-transaction costs could severely crimp issuers' profits, some industry executives say.

"This ruling is going to have a seismic impact and radically reduce profits for large debit issuers, because their cost per transaction is pretty close to zero," says Eric Grover, principal at Intrepid Ventures. "If the ruling sticks, tens of billions of dollars in interchange revenue will evaporate"

Grover supports Traynor's ruling even though he opposes the Durbin Amendment. That's because the Fed did not faithfully implement the law's "purposefully punitive debit-interchange price caps," he says. "Congress, not the Fed, is the policymaker," Grover adds. "The Fed's job was to implement Congress's intent as expressed in the text of the statute."

Under rate caps imposed by the Fed in 2011, Mastercard and Visa issuing banks with at least $10 billion in assets can charge up to 21 cents per debit card transaction, plus a penny for fraud prevention and 0.05% of the transaction for fraud-loss recovery. While the Fed's rate cap cut the interchange revenues of big issuers by about 50%, merchant groups have long argued the caps do not reflect the actual per-transaction cost to debit card issuers, which is 3 to 4 cents and can be even less for the largest issuers.

"The judge basically told the Fed that debit rates need to be calculated in a more straightforward way," says Stephanie Martz, chief administrative officer and general counsel for the National Retail Federation. "Judge Traynor did a very good job of establishing that the Fed included a lot of costs in setting the caps that violate the Durbin Amendment."

While the Fed opted to review the rates caps in 2023 and asked for industry input, that move was essentially a non-starter with merchants. They felt the central bank's decision was motivated by a decline in other costs associated with debit transactions, rather than a decline in interchange.

"That proposal didn't correct the original mistake, which was looking


Grover

Grover: "This ruling is going to have a seismic impact and radically reduce profits for large debit issuers."

at the entire cost structure of debit acceptance, not just the actual cost per transaction," says Doug Kantor, an executive committee member at the Merchants Payment Council and general counsel for the National Association of Convenience Stores. "[Traynor's] ruling also supersedes the Fed's 2023 proposal."

Now, large debit issuers are expected to see their revenues severely crimped as a result of Traynor's ruling. But Capital One is a potential beneficiary thanks to its acquisition of Discover Financial Services earlier this year. Discover, which issues both credit and debit cards, is exempt from the provisions of the Durbin Amendment as a third-party network that competes with the Visa and Mastercard networks.

"Discover issues debit cards, and there are very few of them in circulation, but Capital One now issues them, which gives Discover an enormous advantage [under Durbin,]" Grover says. "Capital One can use the higher revenues it can earn under the terms of the ruling to fund incentives that can attract cardholders that banks affected by Traynor's rulings can't."

Traynor also issued a hold on his decision, pending any appeals, to prevent any market chaos that could result from immediately dispensing with the Fed's rate caps and creating an unregulated market in which debit issuers could set interchange rates as they see fit.

"With the hold in place, the current rules regulating debit interchange remain while the appeals process plays out," Kantor says. "Without the hold, the debit ecosystem would jump into the unknown of no regulation."

Traynor's ruling may well be appealed, but the odds of success are poor, even if the appeal reaches the United States Supreme Court, some observers say. "The Fed has exceeded its authority by taking [on] too much discretion in its interpretation of the Durbin Amendment," Grover says. "If the ruling is appealed to the Supreme Court, it would probably agree with Traynor's ruling."

— Peter Lucas

FAST FOOD POS CAN BRING ON FAST HEADACHES

Having fought back from the ravages of the pandemic, quick-service restaurants now represent a large and fast-growing market for providers of point-of-sale technology—but also one presenting new and vexing challenges, according to top payments executives who specialize in this industry.

For fast-food or fast-casual restaurants, "building a point of sale today is a very different proposition from what it was a few years ago," said David Burkhart, vice president for enterprise clients at Lombard, Ill.-based POS provider QSR Soft. QSR is an industry abbreviation for quick-service restaurant.

For one thing, system complexity, which was always challenging, has only grown more so, noted Burkhart and a panel of other payments executives who spoke late July at the annual meeting of the Midwest Acquirers Association in Chicago. For some panelists, this creates a fast-growing challenge not just for restaurants but for the companies supporting their payments flows. "When you're dealing with millions of lines of code, things are going to break," noted panelist Bryan Solar, chief product officer at SpotOn, a San Francisco-based POS technology provider.

For Solar, that means companies like his must be prepared to spend more than ever on research and development—not just to improve technology but also to be prepared for system failures. "We are spending millions on R&D," he told the audience. "You have to have a lot of money to make these bets and have them go wrong." The U.S. restaurant industry as a whole is expected to spend just over $10 billion annually on POS technology alone by 2030, up from nearly $6 billion in 2022, according to estimates from Grand View Research.

For Solar and the other executives on the panel, though, the need for such investments is sharper than ever, at least in part because of growing complexity. "In any QSR in America, chances are there's more redundancy than there is on an airplane," noted Chris Siefken, president of Restaurant POS, part of the big Atlanta-based payments provider Global Payments. "The customer expectation is that it's just going to work."

When it doesn't work, the POS companies often get the blame, regardless whether the source of the issue lies elsewhere in the system, the executives said. “We’re the face of the problem,” said Siefken. But the restaurant faces a backlash, as well. “This is going to be on CNBC,” noted Siefken. “We’ve got to get that operation up as soon as we can. The impact on that operator is going to be very large. Margins are very thin.”

To avoid that kind of heat, systems installed only recently require constant updating, the panel cautioned. “Somebody has to be on call. It’s a big deal,” said QSR Soft’s Burkhart. That’s because a system failure means loss of income for what is often a slim-margin business—an outcome that potentially impacts outlets’ managers and employees, the panelists said. “These are peoples’ businesses, their living. One single day can cause that problem,” noted Siefken.

But the opportunity for service and support can be attractive, despite the reputational risks a system failure presents. Said Solar: “Any business owner who buys a POS is not buying it for today, he’s buying it for the next 15 to 20 years.”

— John Stewart

FORTER, IDENTITY MONITORING, AND AGENTIC COMMERCE

Identity-intelligence platform provider Forter has launched a service that it says enables digital merchants to vet AI agents across the entire shopping process, including payment.

The new capability within the Forter platform is intended to help merchants combat fraud in the era of artificial intelligence, which has seen the rise of AI agents that perform tasks ranging from product discovery to offering personalized product recommendations to shoppers.

The new service, which Forter says is the first in a series aimed at helping digital merchants build trust in AI agents, can detect when a consumer is engaging in AI-assisted shopping and differentiate malicious AI agents from legitimate ones. The app can also distinguish different types of AI agents, such as reflex- and goal-based agents, and AI agents that learn.

Criminals have been rapidly adopting AI agents to commit fraud, launch malicious attacks against businesses, create fake consumer accounts, take over accounts, and masquerade as legitimate AI agents.

“AI has lowered the barrier to fraud entry. It is no longer just career criminals or sophisticated hackers. Anyone with intent can now use AI-powered tools to commit fraud across the customer lifecycle,” says Cyndy Lobb, Forter’s chief product officer. “From account creation and takeovers to purchases and returns, we are seeing a surge in automation being used to exploit weaknesses at scale.”

Criminals are using AI agents to create synthetic identities that can bypass traditional fraud detection, test stolen consumer credentials, and submit fake claims for refunds at scale. Such tactics are disrupting the consumer-merchant relationship by making it harder for merchants to understand a shopper’s intent. That’s a problem because the e-commerce model is built on a direct connection between brands and individual consumers or households, according to Lobb.

“Many of today’s product, marketing, and merchandising decisions are based on customer behavior and purchase patterns, Lobb says. “If agents are inserted into the flow, those signals can become distorted or incomplete. For large platforms with retail media networks, the impact can undermine ad targeting and attribution tied to known customers.”

The use of AI agents by criminals also makes it harder for merchants to verify identity and

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.**

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

Chargebacks Transactions % of Transactions - Chargeback number divided by bankcard + OptBlue transactions

Q1’24	0.033%
Q2’24	0.029%
Q3’24	0.031%
Q4’24	0.030%
Q1’25	0.030%
Q2’25	0.027%

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

personalize consumer experiences, Lobb adds.

Helping fuel criminals' use of AI agents is that the technology is rapidly becoming popular with online shoppers. Within the next five years, AI agents are projected to be generating 20% of consumer-driven digital traffic, according to Gartner. In addition, Forter says it has seen a 50% increase in fraud using scripted and automated attack modes, which can be carried out by AI agents to rapidly change identities and manipulate images.

"AI agents are being adopted to enhance the customer experience by making product discovery, comparisons, and transactions faster, seamless, and more personalized," Lobb says. "As these tools become more accessible, they're transforming how shoppers engage and enabling new opportunities for brands to increase loyalty, repeat purchases, and customer satisfaction."

Looking ahead, Forter plans to release services that use multiple agents for automating policies, build insights into behavior trends across the customer base, and provide agentic tokenization.

— Peter Lucas

PAYPAL'S GAMBIT TO AVOID WALLET CONFUSION

PayPal Holdings Inc.'s latest wallet initiative, PayPal World, will go live this fall and aims to reach more than 2 billion consumers, the company's chief executive said late in July. Alex Chriss followed up on an earlier announcement of the initiative by stressing how the venture will tie together five of the largest digital wallets from around the world, including Mercado Pago, Tenpay Global, and UPI, as well as PayPal and Venmo.

"It's five of the largest wallets in the world coming together on a global platform," Chriss told equity analysts during a call to discuss PayPal's June-quarter results.

The initiative, Chriss said, is aimed at stitching together what the partners see as a fragmented market globally for digital-wallet coverage. For the consumer, this fragmentation means "you're never quite sure where your wallet will be accepted," he said, "so the merchant needs to accept dozens of wallets."

The confusion of wallets could get worse quickly, Chriss said. Altogether, some 3.5 billion people worldwide "rely on digital wallets," a number that will grow to 5 billion by next year, he said. The initiative will also include stablecoins, he noted, a move that follows recent action by the United States to sign into law a bill setting out regulations for the cryptocurrency. The GENIUS Act is expected to stimulate faster growth for stablecoins by clarifying what the government will tolerate.

Now, PayPal is looking for faster growth in digital currency. The company in July announced Pay With Crypto, an initiative Chriss said will let PayPal "tap into a base of 650 million cryptocurrency holders" globally. "It's a big part of U.S commerce and will be onchain," he noted.

Chriss noted another development related to digital wallets by celebrating results for the Venmo peer-to-peer payments service. "There's something magical happening with Venmo," he noted. "The team is really killing it." Total payment volume for Venmo grew 12% in the quarter, up from 8% in the same period last year and from 10% in the March quarter. The product is now growing at "the highest rate in the past three years," PayPal said in charts accompanying Chriss's presentation.

"The question was, Can you grow Venmo?" Chriss noted. "The answer is yes." Moves to capitalize on Venmo's popularity include recent agreements with universities in the Big 10 and Big 12 athletic conferences to let students use the payments service with cobranded Venmo cards. "The user base is not just growing, it's engaging in commerce," Chriss said.

For the June quarter, PayPal reported $8.29 billion in revenue, up 5% from the same quarter in 2024, on $443.5 billion in total payment volume, up 6%. Transactions came to 6.23 billion, down 5%. Active accounts added up to 438 million, up 2% year-over-year, Branded checkout volume grew 5% in the quarter, "despite tariff headwinds on retail spending," the company noted.

— John Stewart

SIGNAPAY | PAYLO

Wake up *WINNING*

—with the Confidence to Close More Deals

Tools, tech, and training that give you the edge.

From PayLo Dual Pricing to Empower U's real-world training, SignaPay gives you everything you need to sell smarter, close faster, and lead with confidence.

Your *WINNING EDGE*

- *Higher residuals*
- *Custom Payout Programs*
- *Loans & Residual Buyouts*
- *Best in class CRM*

Your *CONFIDENCE BOOST*

- *Quick & easy lessons with EmpowerU*
- *Personalized Sales Office Support*
- *Build Customized Downlines*
- *Designed for agents who want to win*

Train Smarter. Sell Faster.

Empower U: Your Shortcut to Sales Mastery

With Empower U, you get more than training—you get the playbook for winning. Learn proven sales tactics, master complex topics like dual pricing, and walk into every meeting ready to close.

One partner. Unlimited potential.

Start closing more deals today.

paylo.signapay.com | 877-231-6609 | partners@signapay.com

THE EVER-PRESENT PRIVACY CHALLENGE

BY
GIDEON SAMID
gideon@bitmint.com

"TELL ME WHAT you are buying and how much you are paying, and I will tell you what you are thinking of, what you wish for, what your plans are."

Our payment profiles, chewed on by artificial intelligence, serve as an open window to our most intimate whims and desires, whether we are payment card-using individuals or a large multi-component organization. Even our financial meta data (financial data without the amounts being revealed) are a rich source of intelligence. Much of it is collectible from public sources, which makes their analysis perfectly legal.

Indeed, we are witnessing a blossoming industry where "gray hackers" offer their clients critical intelligence regarding their competition. The original allure of Bitcoin was its hailed privacy, yet now the battle over our private data involves digital money and advanced cryptography.

The cause of privacy has recently been augmented through content-discriminating ciphers. A normal cipher transforms a plaintext message (payload) into its encrypted version and then reverses the process at the receiving end. A content-discriminating cipher also encrypts the payload, but then arms (combines) the resultant ciphertext with "fakeload," turning it into an "armed load." The recipient of the armed load will readily discriminate between the payload and the fakeload, but an eavesdropper will face the full range of possibilities from zero fakeload to zero payload.

Two financial institutions engaged in a pattern of mutual payments will carry out these payments through such content-discriminating ciphers. They will establish a fixed flow rate of data in both directions. If no payments are made, the flow will be consistent with a fake data flow and will be so identified by its recipient. Should a payment occur, it will manifest itself as a proper payload that fits into the ongoing data stream, and will be identified as such at the receiving end. Eavesdroppers will see no change, only the same data rate going back and forth.

Content discrimination may be further applied to pack a ciphertext stream with decoy messages designed to deter an attacker from even attempting to cryptanalyze the flow. The fakeload component of a ciphertext is subject to one attribute—being recognized as data that is not to be decrypted, but rather discarded. Alas, by using a different cryptographic key, the roles may be reversed. The original payload turns into a fakeload, and the original fakeload into a payload.

This recalls the story of the seven blind men, each touching a different part of an elephant, each forming a different conclusion as to what the creature is. The same ciphertext stream will be interpreted as two or more distinct—perhaps opposing—messages, dependent on which key is used to read the incoming cryptogram. And since the cryptogram does not reveal which key the recipient is using to read it, there is also no risk that a smart hacker will extract from the cryptogram the right message in the range of all the packed messages, even if the super-smart hacker identifies all the messages that were packed into the ciphertext stream.

Another big boost to the cause of cyberspace privacy comes from "Hidden in Plain Sight" (HIPS) technology. Secret messages are packed into innocent text, which creates the gold standard in cyber privacy. Not only is the content of one's communication protected, but also the very fact that communication took place remains unknown to hackers.

While we all celebrate new tools for advanced financial privacy, we must note that these very tools are serving the dark elements of society, too. The challenge—to achieve balance between lawful conduct and privacy needs—is ever more present. DT

PRIORITY

Celebrating *20 years* of opportunity in every transaction.

Priority's two decades of experience help you accelerate cash flow and optimize working capital so you can grow faster in a competitive market.

Connect with us at booth #408 at WSAA 2025

CELEBRATING

20 YEARS

WHO OWNS THE DATA SHARED THROUGH OPEN BANKING?

BY BEN JACKSON

bjackson@pa.org

A MOONSHINER'S CASE from almost 50 years ago could have an effect on the future of open banking.

In 1973, firemen and a sheriff's department responding to a warehouse fire found a 7,500-gallon-capacity distillery and 175 gallons of whiskey. The problem was no one had paid any taxes on the whiskey.

This led the Bureau of Alcohol, Tobacco and Firearms to subpeona the bank records of the man renting the warehouse. He made pretrial motions to suppress the bank records, arguing they were his private records and protected by the Fourth Amendment.

By 1976, the case had made it to the Supreme Court. In United States v. Miller, the Court held that the bank records were legally subpoenaed and could not be suppressed. The interesting part is why they ruled that way. The Court wrote that "[o]n their face, the documents subpoenaed here are not respondent's 'private papers.'... Instead, these are the business records of the banks."

Some banks have made similar arguments about handing over records to fintechs through open-banking arrangements. Their argument is that the records are their property, not just consumer information.

The majority opinion in Miller discusses how the checks used by the defendant are not private papers but "negotiable instruments to be used in commercial transactions." This case was decided before the concept of open banking existed, but it is not hard to extend the argument and argue that the information banks hold about their clients' financial activities, at least in part, exist only because the bank itself exists. So, it is not purely customer data.

The Consumer Financial Protection Bureau finalized its first open-banking rule in October of last year. The rule was required under Section 1033 of the Dodd Frank Act of 2010. It was subject to an immediate lawsuit in the Eastern District of Kentucky by banking trade associations. When the new administration arrived in January, it sought to end the lawsuit by announcing that it would vacate the rule.

The courts granted the fintech trade associations permission to keep fighting for the rule. That an agency is free to rewrite its own rules didn't seem to matter at the time. But in response, the CFPB asked and received from the district court a motion to stay the proceedings while it writes a new rule.

In its request on July 29, the Bureau said it would "engage in an accelerated rulemaking process" and have a revision in three weeks. It left itself some room by saying that it planned to engage with the public and that it would file status reports every 90 days. So, it seems they expect there could be delays.

One major issue the new rule needs to address is whether and how much banks can charge for access to their data rather than being expected to pay to build systems to help competitors take data out of the bank. Chase started the negotiations when it announced it would begin charging fintechs for access to its system.

While the Miller case can't completely resolve the questions around this later case, it does provide a starting point for the banks to argue they have an ownership stake in the information the fintechs want them to provide.

Other issues will fall outside the ownership question, such as how much liability data providers will have once they share the data and how soon they must delete the data they request on behalf of the customer. But by establishing their stake in that data, financial institutions can make an argument for more controls on sharing it. DT

HOW OPTIMIZING PAYMENT STRATEGIES CAN FIGHT INFLATION

Here's how small merchants can mitigate the effects of rising prices while boosting efficiency and pleasing customers.

BY **AUSTIN MAC NAB**

Austin Mac Nab is founder and chief executive of VizyPay.

INFLATION IS A TOP concern of small businesses today. A Q4 2024 U.S. Chamber of Commerce Small Business Index revealed that over half (55%) of small-business owners consider inflation costs the biggest challenge they face. In fact, for almost three years running, inflation has been the dominant concern of small businesses.

In July, the U.S. inflation rate stood at 2.8%, a slight decrease from the 3.1% in January of last year. While inflation has eased, that doesn't mean small-business owners will see an immediate increase in consumer spending or lower prices. With inflation lingering, cost pressures continue to squeeze small businesses, resulting in higher operational costs and reduced profit margins.

As the nation's 34.7 million small businesses continue to grapple with the persistent impact of inflation, they need to adopt new strategies to drive growth. These strategies must reduce costs, enhance consumer experience, and increase efficiencies.

To help achieve this, small businesses can optimize their payment strategies with robust payment-processing technology that:

- Simplifies payment processing and reduces costs;
- Delivers on evolving customer payment preferences;
- Grows with the business; and,
- Focuses on security

Drazen/AdobeStock

CUTTING COSTS

Starting with the first item on that list, small businesses can combat rising costs, the calling card of inflation, by simplifying payment processing. This cost-cutting measure bolsters the bottom line without weakening customer value.

There are various ways payment-processing technology can help small businesses cut costs, including

Sersoll/AdobeStock

transparent pricing, multiple payment options, a cash-discount program, and streamlined integration with existing systems.

The complexity of fees involved in payment processing often results in higher-than-expected costs for small businesses. Transparent and clear information about fees eliminates hidden charges, allowing companies to budget for processing expenses accurately.

Processing technology that allows merchants to accept multiple payment options, including credit cards, debit cards, digital wallets, and online payments, can help businesses cater to the preferences of a wider range of consumers. This can boost revenue by increasing the number of returning customers and attracting new customers.

A cash-discount program is another way to optimize payments. This program integrates processing fees directly into a small business's pricing structure, allowing business owners to offset the costs associated with card transactions, ensuring a more predictable revenue stream. The program treats processing fees like any other cost of goods sold, ensuring that businesses do not lose money every time a customer opts to pay with a credit card.

Lastly, by seamlessly integrating with existing point-of-sale systems, advanced payment technology automatically adjusts prices to include the cost of card-processing fees. This ensures that every transaction is accounted for, allowing for easier transaction management and lower overall processing fees. The technology also provides detailed analytics and reporting, which gives small-business owners a holistic view of their businesses' health and full insight into how much they are saving on processing fees each month.

MORE METHODS

With respect to the second item on the list, offering multiple payment methods to cater to customer payment preferences offers value and convenience. Customers want options. Small businesses also derive significant value from offering a variety of payment options. This value accrues from increased customer satisfaction and loyalty, which can boost overall profitability even in an inflationary environment when consumers are tightening up on spending.

In the digital-first era, people are flocking to frictionless, secure payment methods such as mobile wallets. The growth of mobile payments is enabling businesses to prioritize fast, convenient transactions in-store, online, and everywhere in between. Digital-payment gateways break down geographical barriers, allowing small businesses to expand their market reach, boost revenue potential, and increase consumer interaction.

A McKinsey "State of Digital Payments 2024" report revealed that digital-wallet usage is experiencing rapid growth, increasing from 19% of respondents in 2019 to 28% in 2024. According to the report, 74% of U.S. consumers surveyed indicated easier and faster checkouts as a primary reason for using digital wallets, and one in five digital-wallet users often leave home without their physical wallets, relying instead on digital methods to pay and transact in physical locations.

Even though consumers increasingly use digital wallets, there are gaps in merchant acceptance of this form of payment. A Banking and Payments Intelligence report by J.D. Power revealed that only 57% of small businesses now accept digital wallets, compared with 94% accepting credit and debit cards.

The bottom line is that consumer payment preferences are rapidly evolving, and small businesses must adapt to remain competitive and drive growth.

FLEXIBLE AND SCALABLE

As for payments technology that grows with the business, small businesses need tailor-made payment technology to handle both change and growth. In other words, payment technology that is flexible and scalable.

Mac Nab

Mac Nab: "As the nation's 34.7 million small businesses continue to grapple with the persistent impact of inflation, they need to adopt new strategies to drive growth."

Small businesses also need payment-processing technology that is flexible enough to adapt to evolving technologies and consumer payment preferences and scalable enough to support growing transaction volumes and expansion into new markets.

Flexible, scalable payment-processing technologies futureproof payments for small businesses without compromising on speed, efficiency, convenience, or security. These technologies grow with small businesses without requiring major upgrades or cost increases.

The business landscape is not static, and the payment solutions used by small businesses should not be static, either. Merchants must optimize their payment approach with easy-to-implement, customizable payment solutions that can adapt and scale as their needs change.

FIGHTING CYBERCRIME

Finally, on security, cybercrime is a major concern for consumers regarding digital payments. A Chubb report on the Impact of Cyber Scams on Trust in Digital Payments found that, worldwide, more than 60% of consumers responding to the survey indicated they have altered their behavior or reduced their usage of digital-payment platforms due to concerns about cyber scams or fraudulent activities.

Fraud risk is also a pressing concern for small businesses. Fraud is expensive for merchants, translating to higher credit card processing costs and chargeback fees. A study from Juniper Research forecasts that merchant losses from online payment fraud will exceed $362 billion globally over a five-year period (2023 to 2028), with losses of $91 billion in 2028 alone.

Payment-processing technology is advancing to combat payment fraud with security measures such as AI and tokenization.

AI is emerging as a critical tool for ensuring the security of payment information. AI boosts the speed and accuracy of fraud detection, analyzing transaction patterns for unusual activity to detect fraud in real time. Mastercard noted that AI enhancements boost fraud-detection rates by 20% on average.

Tokenized transactions involve a process that replaces sensitive payment information, such as credit card numbers, with algorithmically generated numbers and letters called a "token." When a consumer taps a contactless card or a phone in a store or to make payments in-app or online, the actual card information is never shared. Tokenized transactions reduce fraud risk, reducing false declines and enhancing the customer experience.

Advanced payment processing technology with strong security can help small business owners secure customer payment information, avoid higher credit card processing fees and chargebacks, and protect their bottom line.

WRAPPING UP

Inflation is a growth inhibitor for businesses. However, optimizing payment strategies with payment-processing technology that simplifies and reduces costs, delivers on evolving customer payment preferences, grows with the business, and focuses on security can help small businesses successfully navigate tough economic times and even drive growth.

A payment-processing partner with transparent pricing that reduces payment complexity and costs, offers the payment options customers prefer and businesses require, and includes advanced security features to combat payment fraud is a partner that small businesses need to remain competitive in good times and in bad times. DT

MAKING PAYMENTS PART OF THE CONVERSATION

Allowing customers to pay via a text message is becoming reality faster than you might have supposed.

BY **DAVE BAXTER**

Dave Baxter is chief executive of Solutions by Text.

TEXT MESSAGING HAS been around for decades. It's a simple tool for connecting. But what's happening right now with the beginning of the widespread adoption of Rich Communication Services, or RCS, is nothing short of a transformation. RCS isn't just about sending better texts. It's poised to fundamentally redefine how payments happen, truly ushering in a new era of conversational commerce.

For decades, businesses have tried everything—phone calls, mail, emails, apps—to reach customers. Frankly, this is overwhelming for consumers. The messages are noise. Consider consumer finance, where people are juggling multiple bills and trying to remember logins for confusing online portals. It's a nightmare, and it leads to delayed or abandoned payments, lower recovery rates, and increased costs for everyone.

123RF/Thanakorn Lappattaranan

If making a payment is too much work, people don't do it. It's that simple.

Modern consumers, especially Gen Z and Millennials, scream for simplicity, speed, safety, and ease when transacting. Where do they want to interact and transact? Right there, in their native texting app. After all, it's the channel they use constantly, all day, every day, for personal communication.

Meeting customers on their phones isn't just a good idea. It's a direct line to engage with maximum impact. You know they're looking at their phones throughout the day.

TEXT AND PAY

RCS is a payments breakthrough. It takes the basic, one-way short-message service and turns those simple texts into secure, interactive experiences. We're moving way beyond just sending a notification. RCS enables secure, branded, and compliant two-way interactions directly within the messaging interface. That means significantly increasing customer engagement.

Currently, text-based solutions demonstrate the sheer potential of embedding the payment process directly into the texting conversation. This means there's not just a link to some external portal you have to log into. No, the goal is to make getting paid just one text away, with no portals and no hassles.

Imagine that you get a payment reminder via text. You then simply respond with a keyword reply to start the transaction. The system confirms the details, asks for your okay, processes the payment, and sends you a confirmation message, all within the native texting app. No app downloads, no portals, or forgotten logins. That's the experience customers want.

Texting doesn't just outperform other channels. It absolutely crushes them. It drives significantly more completed payments because 98% of messages are opened and read within five minutes. This offers unparalleled reach and visibility.

Messages only matter if the audience gets them and knows who they are from. That direct line, that impact, delivers results. We're seeing 2x payment generation compared to mail, phone, and email. Also, this approach lets consumers act immediately, leading to 50% faster payments, and they're 85% more likely to pay on time because of those seamless reminders.

'TANGIBLE BENEFITS'

Texting beats every other channel, five to one, in terms of completion of payment.

The tangible benefits we're seeing today across the entire loan journey underscore the power of this approach:

- **Originations:** Text messaging can dramatically improve loan application completion through timely notifications. This leads to increased loan volume and faster time-to-funding. We saw a 25% increase in application approval to funding conversions as reported by one national lender. Think about the impact of losing 40% of loan-application acceptance rates when not using texting.
- **Servicing:** Providing relevant account updates via text maximizes customer engagement and retention. It streamlines case resolutions and genuinely enhances the customer experience through real-time communication. We've seen call-center time-to-resolution drop from eight minutes to just two minutes using text.
- **Bill Payment & Collections:** Delivering payment options directly to people's phones drives faster payments, reduces delinquencies, and significantly improves recovery rates. Using text for payment-plan reminders reduces broken promises-to-pay. One company saw a 20% reduction. Organizations are achieving a 70% retention rate across all contact channels. This is tangible. This is real.

Overall, leveraging texting for financial communications has demonstrated significant outcomes, including up to a 400% return on investment for texting programs and a 97% reduction in time to revenue. We're talking about reducing chargeoffs by 10%, increasing collection rates, and decreasing day sales outstanding. This is why we are laser-focused on this space.

As RCS adoption becomes more widespread, the potential for payment interactions explodes:

Baxter: "The future of payments is increasingly conversational, and I can tell you, from what we're seeing, effective conversations truly pay off."

- **Enhanced Branding and Trust:** RCS brings verified sender profiles, with business names and logos. In finance, this is crucial for building the trust needed for payment messages. Messages only matter if the audience gets them and knows who they are from.
- **Richer, More Intuitive Interactions:** It goes beyond simple text. RCS supports richer media, suggested replies – making the conversation much more streamlined and user-friendly. It can perform actions comparable to an app.
- **Deeper Embedding of Functionality:** RCS facilitates even tighter integration. We can embed more complex interactions directly within the message thread. Imagine opening a credit card or instantly dropping a virtual card into a mobile wallet via text.
- **Streamlined Service Integration:** Banks can combine payment requests with real-time customer service within the same messaging thread. This transforms a simple transaction into a seamless, full-service conversation, shifting customer interactions away from call centers and toward preferred digital-messaging channels.

This increasing sophistication allows payments to move from a separate, often frustrating task into a natural, intuitive part of the ongoing customer relationship.

'COMPLIANCE FIRST'

Now, let's talk about the elephant in the room: compliance. For us, it's foundational. As conversational commerce continues to evolve, maintaining compliance becomes increasingly critical. In consumer finance, even small mistakes can lead to significant consequences. Any solution delivered via messaging, particularly for payments, must strictly follow regulatory requirements and security best practices.

We purpose-built our platform with compliance at its core. We check user identity, location, time of day, contact history, consent status—that is, whether someone has opted in or out—and the content of each message. It's not easy, but this "compliance-first" approach is essential for building trust and making messaging a viable payment channel.

We see ourselves as a safeguard, helping customers stay on the right side of compliance while navigating complex regulations.

Ultimately, RCS isn't just changing text messaging. It actively transforms the payments landscape by enabling verified, interactive, and compliant transactions directly within the messaging channel. It solves those painful problems with traditional methods and aligns exactly with what modern consumers expect.

Breaking through the noise requires precision, reach, and results. Texting gives you the reach, and RCS delivers precision and that seamless experience, leading to significant, demonstrable results. The future of payments is increasingly conversational, and I can tell you, from what we're seeing, effective conversations truly pay off.

AGENTS OF RISK

Artificial intelligence has had a year to gestate.
Now, as the critical fourth quarter beckons, both good and bad uses of AI are ready to take control of the checkout.

BY KEVIN WOODWARD

As the fourth quarter gets under way, retailers are eager to boost their online sales as much as possible. The risk is that criminals look at the last three months of the year as a bounty, theirs to unlock with all sorts of tools developed to extract the highest yield for themselves.

This year is no different, except that criminals have had a year to refine their use of artificial intelligence tools to help extract that ill-gotten yield. It won't be a free-for-all, however. Merchants, payments companies, and fraud-prevention firms also have had a year to improve their AI tools and clarify how they might use them.

Indeed, preventing online fraud this year will be different. More criminals are using AI, but so too are more merchants and their vendors. Consumers have had another year of exposure to the utility of AI, but may not have caught up to criminal use of it.

And 2025 may mark the first holiday shopping season where AI agents will have a meaningful impact on e-commerce. And that is a complication, though these agents are not automatically obliged to deliver only bad news.

It's no longer a binary decision between a trusted user or one that is a bot or human fraudster. "That's no longer sufficient," says Alisdair Faulkner, chief executive and founder of Darwinium Holdings Inc., a fraud intelligence and analytics firm. "These new AI agents may actually turn out to be your best customers. It's no longer enough to block automated traffic at the front door. The real challenge now is understanding traffic intent."

Faster Fraud

Agentic commerce, according to the consultancy Edgar, Dunn & Co., occurs when consumers enable an autonomous AI agent to browse, select, and purchase products or services on their behalf.

There's no known tally of how many agentic-commerce agents exist, but prominent ones include Perplexity AI Inc.'s Buy Pro. ChatGPT launched its agent in July, and PayPal Holdings Inc. has released developer tools to make it easier to incorporate PayPal payments into agentic-commerce utilities.

AI agents tailored for commerce can operate independently. They can interpret data, understand their shopping environment, and don't need constant guidance, as defined by commerce platform Shopify Inc. Agentic commerce matters for fraud prevention because its automated nature could make it difficult for some detection tools to distinguish when it's being used legitimately and when it's not.

While agentic commerce is set to change how consumers conduct online commerce, so too are criminals ready to employ AI to their benefit.

"The growing accessibility of AI tools has changed the game for fraudsters," says Eyal Elazar, head of market intelligence at Riskified Ltd., a New York City-based fraud-prevention platform.

"On one hand," Elazar continues, "fraudsters are becoming more sophisticated, using advanced techniques like synthetic identities, impersonation scams, including vishing and voice cloning, and emerging tools such as WormGPT to automate attacks. On the other hand, we're also seeing many legitimate buyers referred to our merchants' sites by AI-powered systems like GPT or Gemini."

"Heading into this holiday season," he adds, "the pace of change is speeding up. Agentic AI, which is autonomous AI systems that act independently on behalf of fraudsters, is making fraud faster and harder to detect, requiring fraud teams to adopt more adaptive, real-time detection tools that can analyze multiple identity and behavioral signals simultaneously."

Malicious AI agents mean more sophisticated attacks, says Kristen Kelly, senior vice president of product at Loop Returns, a Columbus, Ohio-based developer of returns-management services.

"We're seeing increasingly sophisticated tactics, with fraudsters using generative AI to mask identities and scale—spinning up new 'customers' with throwaway emails, slightly altered names, and manipulated shipping addresses (e.g., "797 abc N Wall St" vs. "797 N Wall St"). We're already seeing signs of this behavior in the ecosystem," Kelly says by email.

Unhappy Returns

In fact, returns abuse may be one of the more significant ways AI could alter fraud this holiday-shopping season.

"Returns fraud isn't going away, and heading into this next quarter, economic pressures are only mounting," Kelly says. "Because of this, some bad actors are pushing to find more creative ways to exploit return policies. Online shopping has only made this easier, with common schemes including sending back empty boxes, falsely reporting undelivered packages, returning used items, and various forms of social engineering. At the same time, we're seeing more calculated forms of abuse with sophisticated fraud rings leveraging AI to scale operations."

Usually, retailers' reactions to returns abuse is to change policies, says Maanas Godugunur, senior director market strategy at LexisNexis Risk Solutions. That usually leads to an indirect increase in chargeback fraud. More chargeback fraud means more complications for merchants, he says.

AI can have a role in helping merchants counter this, Godugunur says. "The best way we've seen is to always push your customer to a digital channel, even if they came from a call center," he adds. That creates a digital avenue to get a good look at the customer's digital-identity attributes. AI can be injected then to analyze the data and help the retailer make an informed decision, he says.

For example, a look at the digital ID may reveal how many shipping addresses this customer has used. "There's a good-looking digital ID, which usually has one email and maybe one to three devices, usually the [Internet Protocol address] is pretty static," Godugunur says. IP addresses can vary by geography. Maybe there's two shipping addresses. A bad actor will have three or more email addresses associated with it, five shipping addresses, and its IP address keeps changing, he says.

The age of an email also can be an indicator or good or bad intent. "If the age of the email in our global network is less than one week it will lead to a fraud rate of 71% most likely," Godugunur says. Three or more accounts per email could mean an 81% fraud rate.

'Outdated Playbooks'

Another change this year is that criminals continue to innovate. "Cybercriminal organizations are businesses, too, and they care about product-market fit, just like legitimate e-commerce companies. These criminal organizations/businesses are innovating without the bureaucracy that legitimate enterprises navigate," says Frank Teruel, chief operating officer at Arkose Labs, a San Mateo, Calif.-based fraud-prevention firm.

Hall: "The traditional method of manually writing rules and waiting weeks to deploy updates simply can't keep pace with AI-enabled fraud."

Talk to Us
About Our
Personalized Services

Merrick Bank is a proud sponsor of WSAA this year. Connect with us and see how our clients are at the center of everything we do. When you partner with us, **you'll have a team of experts** available to create a specialized program and help you along the way.

- **Top Merchant Acquirer in the U.S.**
- **25+ Years in the Industry**
- **Trusted & Reliable Partnership**

We're ready to design the right program for your business!

Contact us today to set up an appointment.

merrickbankacquiring.com/contact

Merrick Bank®
Merchant Acquiring

Godugunur: "There's a good-looking digital ID, which usually has one email and maybe one to three devices."

Referring to a known instance when bad actors lost out, Teruel says, "When Microsoft disrupted Storm-1152 in late 2023, it took 30 days to reconstitute and it came back even more powerful, using AI to set up fake accounts. Now these attack-automation services are back up in hours, not days, armed with AI. As soon as agentic AI becomes open source, and we believe that will happen in the Q4 or Q1 time period, the fraud floodgates will open."

Storm-1152 was a cybercriminal group that, Microsoft alleged, created approximately 750 million fraudulent Microsoft accounts for sale.

Tactics like these may put more emphasis on the need for nimbleness among merchants and their vendors.

"The traditional method of manually writing rules and waiting weeks to deploy updates simply can't keep pace with AI-enabled fraud that evolves in real time. Companies that haven't embraced machine learning are essentially playing defense with outdated playbooks against opponents using cutting-edge offense," says Alexander Hall, trust and safety architect at San Francisco-based Sift Science Inc.

To get a better sense of their fraud activity, many merchants turn to benchmarking tools, Hall says. That can help understand if fraud spikes are isolated incidents or part of a broader attack. "This contextual awareness wasn't widely available even a year ago."

'The Human Reality is Brutal'

While the fourth quarter always brings an increase in fraud activity, uncertainty about the economy may be a factor, too. "Economic uncertainty is a driving force for fraud, because when consumers are hunting for deals, they become more susceptible to scam Web sites offering 'too good to be true' pricing on popular items," Hall says. "The rise of AI-generated fake storefronts makes these scams increasingly convincing."

He expects account-takeover attacks, a long-standing threat, could surge this year because the combination of high transaction volumes and time-pressured consumers creates ideal conditions for account-takeover campaigns.

Elazar also suggests nimbleness in fraud prevention will become more important in the last three months of 2025.

Indeed, the fourth quarter remains the busiest and riskiest season for e-commerce fraud, and this year is no exception. "Fraudsters are increasingly leveraging AI tools and organized networks, from Dark Web forums to social media, to automate attacks and scale abuse rapidly," Elazar says.

"AI enables bad actors to scale operations with minimal effort, creating more convincing fake users and automating fraudulent claims," he adds. "We're also seeing many new fraudsters, fresh to the game, who rely purely on AI tools they've learned from AI itself, using pre-made AI solutions readily available on Dark Web forums."

As always, a big part of fraud prevention is education, for merchants and consumers. "Consumer education has become a critical industry focus. Research shows that while most consumers believe they can identify AI-generated scams, nearly 20% still fall for them," Hall says.

"Merchant education is equally important," he adds. "Many smaller retailers don't understand current fraud trends and may unknowingly enable fraud by agreeing to manual payment processing when customers claim online checkout 'isn't working.'"

There's no denying, too, that merchant fraud-prevention teams are tasked with ever more work. "The human reality is brutal. Most security teams are already buried, and now their job is essentially doubling because they need to start monitoring for agent-based attacks," Teruel says.

One tool to help may be dynamic risk scoring that can distinguish between AI agent behavior and suspicious automated behavior, he says. "The key is understanding the intent and authorization behind the AI agent, not just flagging fast or unusual patterns. Consumers are going to deploy AI agents they trust, and those agents will gravitate toward platforms that authenticate them quickly, not platforms that treat them like threats."

'A Huge Wall of Friction'

However intent merchants may be to address online fraud in the fourth quarter, it appears a reactive stance may not be the primary method. "This year, we're seeing a shift from passive fraud monitoring toward proactive, real-time threat intervention," says Jay Lawrence, chief executive at Equus Compute Solutions, a retailer-focused systems provider.

"Retailers are increasingly deploying edge-based fraud-detection systems that can act instantly, before a transaction clears, rather than after the fact," Lawrence says. "This is especially critical for Q4's high-volume retail season, where even a few minutes of downtime or unchecked fraudulent activity can cost millions."

vrvirus/123RF

"Compared to 2024, there's a stronger emphasis on distributed intelligence—placing detection and response capabilities closer to the edge, where transactions and customer interactions actually happen," Lawrence adds.

The 2025 fourth-quarter shopping season may be an indicator of how the consumer experience is changing.

"This Q4, merchants need to shift from rigid rule sets and black-and-white logic to more nuanced, real-time risk assessments based on behavioral signals and journey context," says Darwinium's Faulkner.

"Otherwise," he adds, "they risk either letting in sophisticated fraud or alienating legitimate customers who are simply adopting new ways to shop. We don't want consumers to be faced with a huge wall of friction just because they're using the latest tools to buy and sell online. The fraud fight has evolved, and so must the customer experience." DT

Faulkner: "It's no longer enough to block automated traffic at the front door. The real challenge now is understanding traffic intent."

ADAPTING TO VOLATILE MARKETS WITH 'LONG TAIL' THINKING

How crises like Covid, and now perhaps tariffs, can be catalysts for business-to-business payments innovation.

BY **ALLEN BONDE**

Allen Bonde is chief marketing officer for business-to-business payments provider TreviPay.

STORMY TRADE WINDS, political uncertainty, protectionist policies, and talk of a global recession are swirling around us. While we are unlikely to be heading toward upheaval of Covid-19 proportions, the signs of economic turbulence are unmistakable.

These topics came up at a recent Crossroads salon, where a senior economist from a major insurer highlighted the sharp rise in U.S. tariffs from 2.5% to more than 20%, the highest in a century. As the economist pointed out, "Unprecedented U.S. tariffs are slowing global growth, while Europe sees some bright spots with German investment. Businesses must adapt to survive this volatile landscape."

123RF/galexs

While the current situation is undoubtedly concerning, we have weathered significant challenges before. Many organizations used the Covid crisis not merely to adapt, but to rethink their operations, reinvent their models, and build lasting resilience. In times of uncertainty, it is those businesses that embrace innovation and demonstrate resilience that ultimately endure and thrive.

During Covid, businesses quickly realized they couldn't operate as they had been and made a decisive, significant push into digital infrastructure. McKinsey famously reported that companies achieved three to four years' worth of digital transformation in the first six months of the pandemic—in customer experience, supply chains, and internal operations.

Why? Because the urgency of the moment cut through bureaucracy and drove a sharp focus on immediate problem-solving and bold, swift action. McKinsey found respondents expected most of these changes to be long-lasting, and were making the kinds of investments to ensure they were on a long-term path for success.

Tariffs may serve as the immediate pressure point, but the broader opportunity remains consistent: to fundamentally reimagine how we operate, how we sell, how we serve our buyers, and how we cultivate loyalty, namely fostering long-term, mutually beneficial relationships that extend well beyond the traditional vendor-customer dynamic.

MITIGATING DISRUPTIVE EFFECTS

Now is the time to support customers in formulating practical responses to today's most pressing questions: What is unpredictable and beyond our control? What is unpredictable yet manageable? And, perhaps most important, what is relatively predictable and well within our capacity to address?

In my view, the emerging economic division and the repercussions of current U.S. economic policy distinctly align with that third category. While we are unable to prevent the imposition of tariffs, we can strategically prepare for the disruption.

During the pandemic, while working as an analyst at Forrester Research, I interviewed key industry players across airlines, manufacturing, and retail to understand what set leaders apart from laggards. From these conversations, three traits stood out: adaptiveness, creativity, and resilience. Building on these insights and other recent research, and integrating our research on buyer-seller loyalty, we developed the "Long TAIL" framework: Trusted, Adaptive, Intelligent, and Localized.

Let's look at each element of the framework in turn.

Trust is the cornerstone of B2B commerce. Our recent study with 300 B2B buyers in the U.S. and U.K. found trust was the top factor when choosing suppliers—outranking price and payment terms.

At the recent salon, an e-commerce leader from a major hardware manufacturer summed it up: "We know that trust scales much better than features. We can build that trust on a basic service, and that's going to be far more healthy than doing lots of [product] features."

In uncertain times, building trust must be your focus. Strengthen relationships by checking in regularly, understanding how customers face challenges like shifting supply chains or inventory issues, and going beyond with real solutions. Show commitment with real solutions, such as credit flexibility or rapid onboarding for new buyers. "Ready credit" to stock up can boost agility and signal you're in their corner. Be the partner who steps up and says, "We see your costs rising, and we're here to help."

BOLD PIVOTS

Remember how airlines swiftly pivoted passenger routes into cargo operations during the pandemic? Or how retailers transformed stores into distribution hubs? These adaptations and responses were only possible because players had built flexible infrastructure, that is, systems capable of adapting to new challenges rather than being so rigid they couldn't experiment in tough times.

McKinsey's research on digital transformation revealed not only a significant acceleration in the adoption of digital technologies during Covid, but also a remarkable increase in the share of digital or digitally enabled products in company portfolios—jumping ahead by an estimated seven years over that period.

The same holds true today. Those who can quickly adjust pricing, offer trade credit, and streamline onboarding will be best positioned to capture market share. Order-to-cash workflows, in particular, offer huge potential. McKinsey found that every $1 invested here can yield up to $6 in returns.

Whether you're a consultant in this space or simply looking for concrete ROI, this is where to focus your efforts.


Bonde

Bonde: "By nature, a crisis rewards bold thinking and punishes complacency."


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.omeda.com/dtr/
or email publisher Bob Jenisch at
Bob@digitaltransactions.net

THE AI IMPACT

The widespread accessibility of AI has changed the game. Tools like ChatGPT, Google NotebookLM, and specialized AI assistants now empower companies to map buyer journeys, analyze how deals have shifted pre- and post-tariff, and pinpoint opportunities for optimization or protection using AI and GenAI.

By uncovering friction points—such as pricing thresholds, sourcing changes, abandoned carts, and more—businesses gain crucial insights to intervene where it matters most, easing challenges before they escalate.

This is especially vital in embedded finance. As payment expectations evolve, frictionless experiences aren't just a nice-to-have. They're the new baseline.

LOCAL PARTNERS

During the early days of Covid, businesses quickly realized the risks of relying too heavily on single-region sourcing. We're likely to see similar shifts now. A recent Gartner survey found that 51% of global supply-chain leaders believe they could regionalize at least 25% of their supply chain within 12 months, if needed.

Localization can be a powerful strategy. But it's more than just cutting costs or speeding up shipping. It's about building trust through proximity. Nearshoring and supplier diversification reduce geopolitical risks and increase agility.

There's also a psychological advantage. Buyers tend to trust suppliers who are nearby or culturally aligned. Whether it's speaking the same language or sharing similar values, that closeness breeds confidence.

But beware. Localization isn't easy. For example, a Chinese e-commerce site requires more than just translation. It demands different formatting, detailed product info, and authentic local reviews to truly resonate.

In summary, experience shows that both businesses and consumers are remarkably adaptable. So, let's take those crisis-driven lessons and use them to adjust to the new normal, while also seeking opportunities to accelerate innovation and revive transformation projects that may have been sidelined.

By nature, a crisis rewards bold thinking and punishes complacency. Let's not waste this opportunity!

IN A HARD ECONOMY, LEVERAGE A SUBSCRIPTION MODEL

Here's how subscription payments can be a key contributor to building loyalty, reducing churn, and boosting cash flow.

BY **TIFFANY JOHNSON**

Tiffany Johnson is chief product officer at NMI

IF YOU ARE a merchant, sell to merchants, or have a friend who is a merchant that sells subscriptions or recurring services, then this article is for you.

When money is tight, businesses can't afford to let revenue slip through the cracks, but that's exactly what happens when subscription payments fail. Today's consumers love the ease of "set it and forget it," whether it's for their favorite streaming service, meal kit, or fitness app. Yet, every month, thousands of subscribers drop off, not because they want to cancel, but because of payment issues.

The impact is staggering. On average, 7% of all recurring charges fail on the first attempt, and their effect is even more pronounced on subscription orders, most of which are entirely avoidable. That's not just churn, it's preventable revenue loss.

In an uncertain economy, businesses must do more than offer convenience. They must ensure every renewal sticks. The subscription economy is a shift from ownership to access, where businesses thrive on recurring relationships instead of one-time transactions. Recurring revenue and subscriptions are critical for a successful business, so how do you do them right?

POWER AND GROWTH

The subscription economy is booming. Despite economic uncertainty, the subscription model continues to thrive, projected to reach $900 billion by the end of 2026, according to a report from the Business Research Company. Companies love subscriptions because they create predictable, recurring revenue. But what happens when those recurring payments fail? That predictable revenue stream suddenly isn't so predictable anymore.

Consumers love convenience, businesses love predictable revenue, and the model itself has become a dominant force in industries from entertainment to SaaS, retail, fitness, and even automotive. But there's a catch. While subscriptions offer stability, they also come with a hidden risk: payment failures.

It's not customers intentionally canceling. In fact, the subscription model is hugely popular among Millennials (69%) and Gen Zers (66%), according to a report by NMI. These groups prefer recurring payments for frequently used goods and services.

It's credit card expirations, fraud flags, insufficient funds—small things that add up to big revenue losses. The key to success in this space isn't just signing up subscribers, it's keeping them. And that starts with optimizing how you handle payments.

MORE RECURRING BILLING, LESS INVOLUNTARY CHURN

One way for companies to reduce involuntary churn and ensure their payments strategy is working is to use network tokens—secure, tokenized versions of card numbers issued by the card networks and stored by the merchant or payment provider. Unlike static card numbers, these tokens are automatically updated when a customer's card is reissued or expires, ensuring stored payment details stay current.

Network tokens also help prevent fraud and reduce disputes, as card issuers trust the process in which tokens are created more than they do transactions with one-time card entry. As a result, these tokens minimize declines and boost authorization rates. If you're in the subscription business and not using network tokens, you're leaving money on the table.

Timing is everything when it comes to payments. Even with tools like network tokens in place, transactions can still fail for reasons like insufficient funds or temporary issuer holds. That's where smart-retry logic comes in.

Instead of retrying a declined payment at random, this approach uses artificial intelligence to pinpoint the best time for a second attempt, factoring in patterns such as payday cycles, past issuer responses, and customer behavior. Another simple but powerful tactic is sending pre-expiration notifications, giving customers a chance to update their details before a card expires. Together, these strategies can significantly reduce failed transactions and keep recurring revenue on track.

> If you're in the subscription business and not using network tokens, you're leaving money on the table.

MEETING DIVERSE CUSTOMER NEEDS

Beyond preventing failed payments, businesses need to offer payment flexibility. Customers today expect control over how and when they pay, so the days of rigid, one-size-fits-all subscriptions are fading. For example, not all subscriptions should be monthly. Some customers prefer usage-based, pay-as-you-go, or hybrid models. Also, digital wallets and Buy Now, Pay Later (BNPL) are gaining traction. The more payment options you provide, the easier it is for customers to pay in a way that works for them.

Finally, people want the ability to pause, upgrade, or modify their subscriptions without friction. The more control customers have, the more likely they are to stick around instead of canceling outright.

Imagine this: You're sitting on your couch after a long week. You're excited to kick your feet up and binge-watch your favorite show. You earned it. You open the app, but instead of your show, you get an error message: "Payment declined. Please update your payment method." You sigh, thinking, 'I'll do it later.' But later never comes, and, instead, you decide to check out a competitor.

Just like that, the streaming service lost a paying subscriber—not because you wanted to leave, but because your credit card interrupted the experience. Every month, troves of customers—who actually like your product—disappear because of payment failures like this.

At the end of the day, payments are not just a back-office function. They're a critical part of the customer experience. If you optimize them, you're not just reducing churn, you're also building loyalty and improving cash flow. This, in turn, will feed into long-term business success. DT

MAGTEK
SECURITY FROM THE INSIDE

Where Imagination Meets Innovation

Magensa Unigate for ISVs and Developers.

Empower your app to support mobile ticketing, secure access, and concession payments in one seamless experience.

Images are simulations of what is possible. Please contact a representative to see how we can help bring your ideas into reality.

Deliver peace of mind with one rugged, kiosk-ready device, the DynaFlex II PED. Accept tap, dip, swipe, scan, and mobile entry. Your payment app can enable ticket acceptance through Apple VAS and Google Wallet, create loyalty programs with secure tokens, and accept payments at the point of interaction. Payments, access, and authentication simplified.

Built with Qwantum Security, PCI PTS 6.x SRED compliance, tokenization, AES-256 encryption, and DUKPT key management, your solution stays secure so customers can skip the lines and go straight to the magic.

Learn More About
MagTek & Magensa's
Retail Solutions

562-546-6400 | sales@magtek.com | www.magtek.com