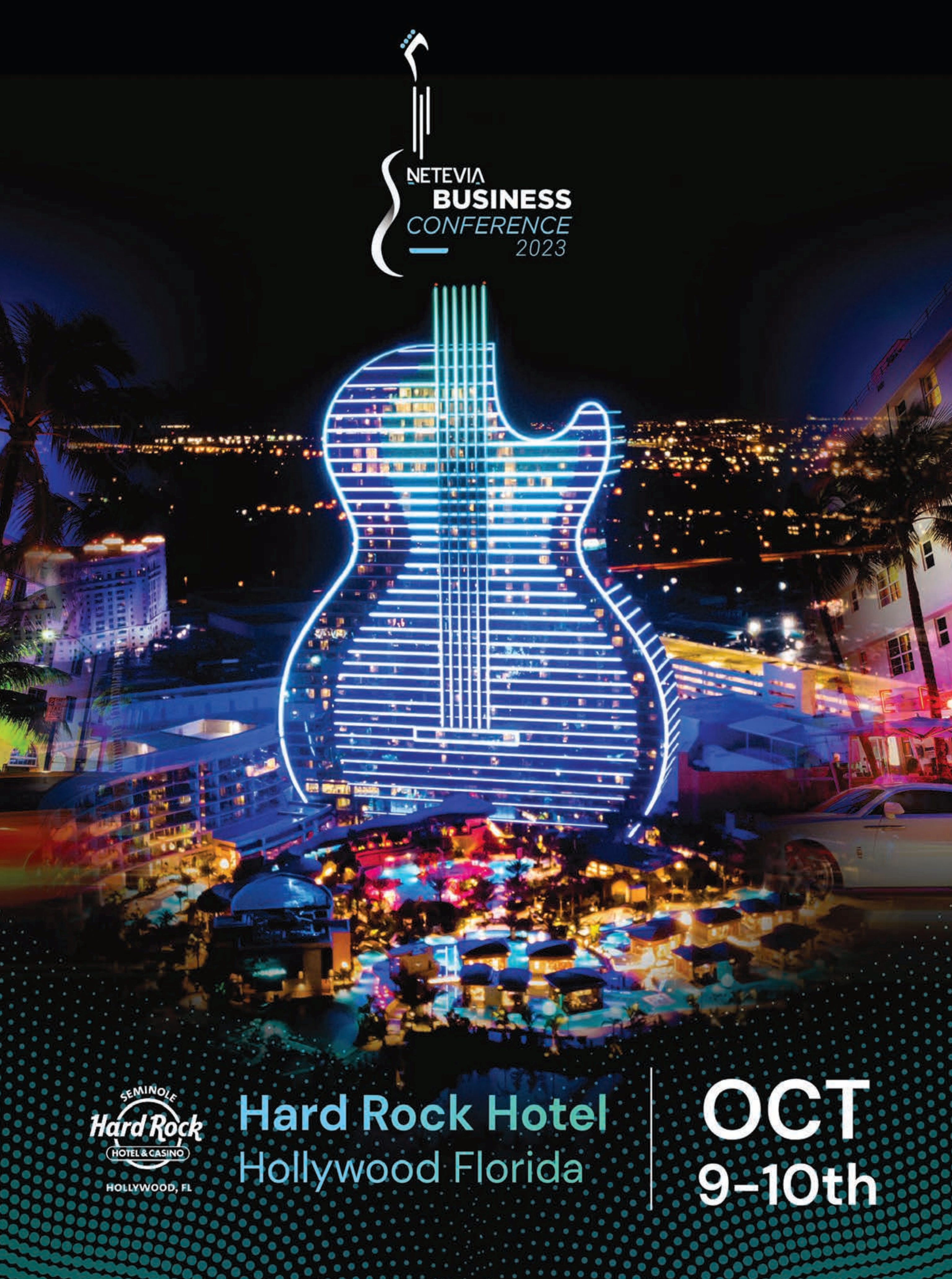
DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

WHO WILL ROUTE TRANSACTIONS?

Legislation like the Credit Card Competition Act may be all well and good—but what alternatives will compete with Visa and Mastercard?

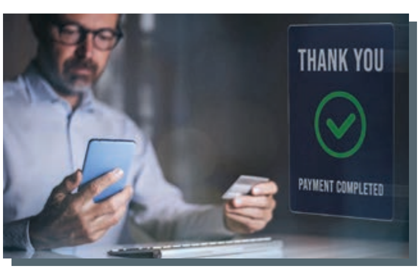
Volume Twenty, Number Nine • DigitalTransactions.net • September 2023

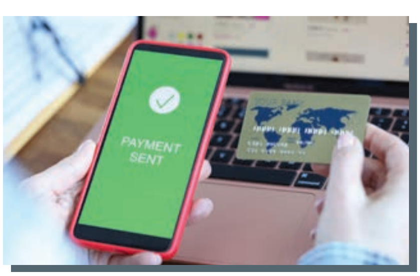
ALSO IN THIS ISSUE:


NETEVIA
BUSINESS
CONFERENCE
2023
SEMINOLE
Hard Rock
HOTEL & CASINO
HOLLYWOOD, FL
Hard Rock Hotel
Hollywood Florida
OCT
9–10th

contents

SEPTEMBER 2023 • VOLUME 20, NUMBER 9





Cover Illustration: Elizabeth Novak, 123rf.com

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.

MAGTEK®
SECURITY FROM THE INSIDE

SECURE ONLINE TRANSACTIONS

Magensa's OmniChannel Service Solutions
DELIVERING SECURITY FOR ECOMMERCE

Watch DynaPAD video

Shop confidently this back-to-school season with Magensa's comprehensive security solutions for eCommerce. Our cutting-edge solutions safeguard every online transaction, ensuring your personal information and payment details are protected. From secure hosted payment pages to transaction tokens, we provide the utmost versatility for online retailers to create a seamless and secure payment experience for their customers. Trust Magensa to safeguard your transactions and enjoy worry-free shopping, making your online journey safe and smooth.

Magensa TokenExchange Payment Gateway Solutions

- Safeguard sensitive payment data with our robust tokenization services
- Transaction Tokens for eCommerce, invoicing, and manual entry
- Connect to leading US payment processors and other gateways
- Enhance security and customer trust with secure hosted payment pages

DynaPAD Secure Card Reader Authenticator and KeyPad

- Durable and secure magnetic stripe reader (MSR) with keypad
- Empowering seamless card present and card not present transactions
- Long swipe path for magnetic stripe cards, an easy-to-use keypad for manual entry of card data, and perfect for call centers

MagTek, Inc.
1710 Apollo Court
Seal Beach, CA 90740

FIND OUT MORE

562.546.6400
sales@magtek.com
www.magtek.com

the gimlet eye

DISCOVER MAKES A MISTAKE

THERE ARE SERIOUS MISTAKES, and then there are the really serious mistakes you can't recover from if you're the top honcho. Discover Financial Services proved that last month with the departure of Roger Hochschild, who had been an executive at Discover for 25 years and chief executive for five.

Discover announced Hochschild's departure weeks after the card network's disclosure in a July earnings call that it had set aside $365 million on its balance sheet to compensate merchants and acquirers that the network had been overcharging for transactions. The practice, which involved misclassification of certain cards into higher-rate tiers, dated as far back as 2007, company executives said on the July call.

Exacerbating the circumstances around this disclosure is that card-acceptance fees for credit and debit are historically a sore point for merchants of all sizes. The issue has been on the boil lately, leading to legislation now before Congress that would require issuers to make two unrelated networks available for credit card transactions. One of the networks can't be Visa if the other is Mastercard, and vice versa. The legislation has far-reaching implications, especially for networks like Discover. For more on this bill, called the Credit Card Competition Act, see our cover story on page 24.

In this sense, Discover's disclosure couldn't have come at a worse time for opponents of such would-be legislative solutions to the acceptance-cost issue. Industry experts, indeed, doubt the management shakeup, coupled with the compensation allowance, will placate merchants. "It's a hot, hot [topic], and somebody has to go on the chopping block," a veteran processing consultant told us, while asking not to be identified. "But I don't think that one sacrificial lamb will be enough. It's another nail in the coffin of interchange." Interchange refers to the percentage of each transaction merchants pay to bank card acquirers and card companies like Discover and American Express.

For its part, Discover's board did not comment on the overcharge imbroglio in announcing the management change. "The board and Roger have agreed that now is the right time to transition leadership" said board chairman Tom Maheras, in a terse statement.

John Owen, a retired banker and member of Discover's board of directors, has been appointed interim chief executive and president while the company seeks a permanent replacement. Time will tell if Owen can help calm the waters in the meantime.

John Stewart, Editor | john@digitaltransactions.net

SEPTEMBER 2023 • VOL. 20, 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, 877-658-0418
bob@digitaltransactions.net

ADVERTISING SALES REPRESENTATIVES
Robert Mitchell, 877-658-0418, x7
bmitchell@digitaltransactions.net

Rob Akert, 877-658-0418, 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 877-658-0418. To subscribe or give us a change of address, go to www.digitaltransactions.net and click on "Subscriber Care" or call 847-559-7599.

BLOCK SQUARES OFF AGAINST MASTERCARD AND VISA

In a major case whose effects could ripple widely across the payments industry, Block Inc. this summer sued Visa Inc. and Mastercard Inc., alleging the global networks worked together to fix interchange fees paid by Block's Square operation.

Square, which processes card transactions for millions of mostly small sellers, pays interchange and other card-acceptance fees on behalf of its mostly small merchants.

San Francisco-based Block's suit comes as the latest challenge—and one of the most substantial—to the networks' longstanding interchange regime.

"Visa and Mastercard have each fixed the Interchange Fees and other fees they charge in connection with the use of credit or debit cards at artificially high levels," the complaint asserts. "Defendants have also engaged in anticompetitive practices that effectively require Square to pay these fixed and inflated fees."

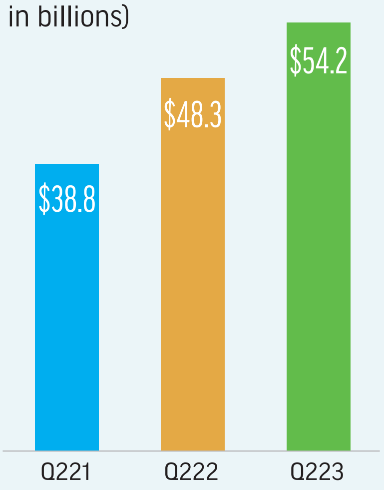
Square processed $46.2 billion in payment volume for its merchants in the first quarter, up 17% from the year-ago period, according to numbers it released earlier this year. In these arrangements, Square is the merchant of record and is responsible for interchange and other fees levied by acquirers and the networks.

A spokesman for Mastercard declined to comment on the suit. Visa did not respond to a request for comment.

Organizations that have long battled the card networks over the costs of card acceptance welcomed Block's action.

SQUARE'S STEADY GROWTH

(Gross payment volume, in billions)



Source: The company

"Swipe fees are far too high and clearly drive up prices for consumers because they're too much for retailers to absorb, especially small businesses. The way they are set by Visa and Mastercard and then uniformly charged by all banks that issue cards under their brands is clearly a violation of antitrust law," says Doug Kantor, general counsel for the National Association of Convenience Stores, in an email message.

Kantor is also an executive committee member of the Merchants Payments Coalition, a group that lobbies on behalf of merchants on payments costs.

Interchange-fee revenue is collected by card issuers, but Block's suit also poses a challenge to another charge—the fixed acquirer network fee, or FANF—that the networks pocket. The FANF, introduced in 2012, aims to encourage more volume by charging less on a per-transaction basis as volume climbs. The fixed fee, however, increases as volume rises into a higher tier.

—John Stewart

THE CFPB AND OCC HAMMER BOFA

Bank of America Corp. this summer again ran afoul of the Consumer Financial Protection Bureau for alleged illicit credit card practices.

In July, the CFPB and the Office of the Comptroller of the Currency announced they were fining the banking giant $150 million for double-dipping on fees imposed on customers with insufficient funds in their account, withholding reward bonuses from credit card holders, and misappropriating sensitive personal information to open accounts without customers' knowledge or authorization.

Under the regulatory agencies' rulings, BofA is liable to pay a total of $90 million in penalties to the CFPB and $60 million in penalties to the OCC, which also found that the bank's double-dipping on fees was illegal. In addition, BofA will pay more than $100 million to customers allegedly victimized by the illegal practices.

After the rulings, a spokesman said BofA had already taken steps to cut or scrub fees, resulting in a heavy hit to fee revenue. "We voluntarily reduced overdraft fees and eliminated all non-sufficient fund fees in the first half of 2022. As a result of these industry-leading changes, revenue from these fees has dropped more than 90%," the spokesperson said in an email message to *Digital Transactions*.

This is not the first time BofA's card business has incurred penalties from the CFPB for alleged deceptive practices. In 2014, the agency ordered

In 2022, BofA took steps to cut overdraft fees and eliminate NSF charges, resulting in a 90% reduction in revenue from those fees, a spokesman says.

BofA to pay its credit card holders $714 million in compensation for what it said were illegal card practices. Other instances cited by the consumer watchdog include unlawful garnishments in 2022, for which the bank was ordered to pay a $10 million civil penalty.

In 2020, the CFPB and the OCC fined BofA $225 million for what they said were "botched disbursement of state unemployment benefits at the height of the Covid-19 pandemic" and ordered the bank to pay hundreds of millions of dollars in reparations to affected consumers.

In its latest investigation, the CFPB says it found BofA had a policy of charging customers $35 after the bank declined a transaction because the customer did not have enough funds in his or her account. The bureau says its investigation indicated BofA double-dipped by allowing fees to be repeatedly charged for the same transaction.

The latest inquiry also found the bank withheld cash and points rewards on credit cards despite its practice of targeting consumers with special offers of cash and points for signing up for a credit card. The bank withheld cash rewards or bonus points from tens of thousands of its credit card holders and failed to honor rewards promises for consumers that submitted in-person or over-the-phone applications, the CFPB alleged.

The bank also denied sign-up bonuses to consumers due to the failure of its business processes and systems, according to the CFPB.

Lastly, the CFPB says BofA misused customer information to open unauthorized accounts in customers' names dating back to 2012. The practice took place to "reach now disbanded sales-based incentive goals and evaluation criteria" for employees, the CFPB says. Specifically, BofA employees illegally applied for and enrolled consumers in credit card accounts without consumers' knowledge or authorization, the regulator alleged.

"Bank of America wrongfully withheld credit card rewards, double-dipped on fees, and opened accounts without consent," said CFPB director Rohit Chopra, in a statement. "These practices are illegal and undermine customer trust. The CFPB will be putting an end to these practices across the banking system."

—Peter Lucas

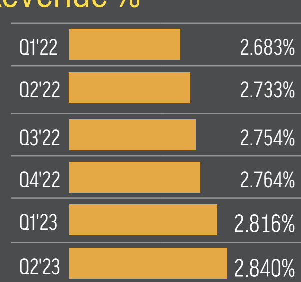
MONTHLY MERCHANT METRIC

Total Gross Processing Revenue %

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

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

Metric Definitions: (Only use definitions related to an individual month's release)
Household - Standalone Merchants are considered as a Household with one store and Chained outlets under a common ChainID are combined together and considered as one single Household.
Total Gross Processing Revenue % - Sum of total discount, total transaction fee revenue and total other fee revenue divided by total volume



tsg

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.

DEBIT NETWORKS FACE A FED CLARIFICATION ON NETWORK CHOICE

Debit card networks are gearing up for an expected flood of new online transactions in the wake of a Federal Reserve rule clarification that took effect in July to require that issuers enable network choice for online as well as in-person transactions.

The latest example emerged last month with an announcement from the Pulse network that it has extended an agreement with Fair Isaac Corp. to use FICO's fraud-analytics technology to support e-commerce transactions in addition to those occurring at store counters.

FICO's technology supports Houston-based Pulse's DebitProtect anti-fraud offerings. Information was not available regarding the length of the contract extension.

The network's move comes as electronic-funds transfer networks react to the Fed's ruling, which the regulator issued in October. The new rule adds no new requirements but makes explicit that issuers must enable network choice for merchants on all debit transactions.

The clarification follows more than a decade after the Durbin Amendment to the Dodd-Frank Act required network choice. Merchants, however, have complained for years that issuers were not observing the rule in the case of card-not-present payments, blunting the amendment's impact and raising sellers' transaction costs.

Instead, many of these debit transactions were flowing to either Visa or Mastercard as issuers feared the higher fraud liability associated with transactions in which the card is not physically swiped or tapped. The new FICO agreement at Pulse is expected to help banks meet the choice requirement by managing fraud risk.

"Our enhanced fraud-detection and blocking capabilities have become more important than ever with the [Federal Reserve's clarification] expected to shift more card-not-present transaction volume to unaffiliated debit networks such as Pulse," said Jim Lerdal, executive vice president of operations at Pulse, in a statement. "Extending our close partnership with FICO enables us to continue enhancing our ability to prevent and respond to the latest trends in debit fraud."

Pulse says 76% of debit card issuers that responded to a survey connected to the network's 2023 Debit Issuer Study had improved fraud models to cut losses and reduce false positives.

—John Stewart

AMAZON SIGNALS A BIG MOVE FOR PALM CHECKOUT

The planned expansion of Amazon.com Inc.'s palm-reading point-of-sale checkout technology to all of the company's 515 U.S. Whole Foods stores, a move the online retailer announced this summer, could represent a major leap for an authentication method few if any other backers have tried.

The technology, introduced three years ago and called Amazon One, is now in use at more than 400 locations, including 200 Whole Foods stores as well as at Panera Bread restaurants and some stadiums.

The Amazon One device allows users to forgo cards or tokens to pay at checkout. Instead, customers authenticate themselves and link to a previously stored card by waving the palm of their hand over the device.

The chainwide expansion to all U.S. Whole Foods locations, which is expected to be complete by the end of the year, will more than double the number of those locations using the technology.

"In a very real sense, Amazon is building an interoperable transaction-acceptance platform that doesn't require anything but the customer's palm once the account has been established. It's a big idea, and with Amazon's penetration of the U.S. consumer base, critical mass will quickly be achieved," notes Thad Peterson, a strategic advisor at the consultancy Datos Insights, in an email message.

To open an Amazon One account, a consumer inserts a credit card into an Amazon One terminal, then waves her palm over the terminal so it can be scanned and linked to the card. Amazon One uses computer-vision technology to select the most distinct identifiers to create a palm signature, Amazon says. Consumers can register one or both palm prints.

Observers point out that the Amazon technology is now well past the trial stage and ready for chainwide adoption. "Amazon One is now a proven technology that effectively eliminates the need for a physical card or digital wallet to enable payment," says Peterson. "The combination of the security of a biometric along with the convenience and speed that the technology offers makes it a logical addition to [the point of sale] for Amazon's captive retail outlets like Whole Foods."

Amazon One: Does its expansion to all Whole Foods stores signal critical mass is fast arriving?

At Panera, which adopted the technology in March, customers who link their MyPanera loyalty account to their Amazon One ID can place an order, receive personalized meal recommendations from Panera associates based on their preferences and previous orders, and reorder their favorite items.

Customers are automatically identified to Panera staff, enabling employees to address a customer by her name. When the order is complete, Panera customers scan their palm again to pay.

In the Panera implementation, first-time Amazon One users can enroll online or sign up when placing an order at a Panera store. Panera customers can link a credit card and their MyPanera account to their Amazon One ID. Customers who have already enrolled in Amazon One at Amazon Go, Amazon Fresh, Whole Foods Market, or other locations where the technology has been deployed, can link their MyPanera account to their Amazon One ID online or in-store.

—John Stewart

AI, MIS-PROFILING, AND A CALL TO ACTION

BY
GIDEON SAMID
gideon@bitmint.com

ARTIFICIAL INTELLIGENCE is profoundly impactful from a payment point of view, probably much more so than we can tell now. What we already foresee is part helpful, part alarming. I will dedicate this column to a particular threat: mis-profiling.

Google's AlphaZero AI machine taught itself to play chess by playing against itself for a couple of hours. It then beat every computer program that had been fed centuries of human wisdom—a stunning milestone. Unlike non-AI computing, AI inference is not comprehensible to humans. Humans can mentally evaluate a handful of factors at any given moment to reach a balanced decision. By contrast, AI can handle myriad details, and use all those details (each one of no great significance) to infer a decision that accounts for all these little pieces of data.

People are impressed by this and learn to trust the machine. After all, AI sees pattern and order where people see chaos and randomness. If privacy-violating central bank digital currency, for example, becomes the way payments are conducted, every one of us will become fodder for AI analytics. That process will reveal subconscious personal goals, passions, proclivities, desires that none of our close ones, nor ourselves, is aware of.

By comparing each of us to all of us, AI profiles the entire payment-using population. We expose almost everything about ourselves through the accumulated record of our payment behavior, day and night, in person and remotely.And AI can—and will—unveil its conclusions to governments.

Even if these profiles are made known to their subjects, there will be no way to contest them, the way we contest credit scores today. This no-recourse feature reflects human ignorance as to how AI draws its conclusions. Now, while AI follows probability calculus and is generally accurate, it is randomly wrong, sometimes very wrong. Countless innocent victims will be denied a loan, a job, school admission on account of what AI said about them.

Let's say you buy a book on the history of political assassinations, and a month later you buy a long-range hunting rifle. You may then fit a pattern that will send the police knocking at your door. Aware of this risk, people will consciously avoid buying items that may lead to logical—but inaccurate--inferences. It is a nightmare out of 1984.

There have been numerous attempts to regulate AI at the inference level. These attempts are mostly articulated by politicians and activists with an insufficient technical foundation. A competent coder can plug into the software stealth algorithmic entities that would bypass top-level regulatory restrictions.

Instead, the best way to tame AI is to control the data it digests. There is a sophisticated way to do this through data contamination, but in this short column I will focus on another tactic, data denial. We have the technology to effect payments on a solid cryptographic foundation that will keep the identities of payors and payees secret from each other, from the bank, and from the government. This technology (one example is BitMint) keeps payment behavior unexposed while offering powerful tools to prevent money laundering.

Alas, central banks lean toward digital money capable of full payment exposure, promoted with shaky assurances of privacy. Central banks have messaging power like no other, including in the United States. Once a digital-coin framework is put in place, it will be too late to uproot it.

This monthly column cannot do much. Yet, maybe these words will stir an enterprising reader to chart a course to preserve that staple of the American way of life—unmonitored payments. DT

FIVE QUESTIONS TO ASK ABOUT AI

BY BEN JACKSON
bjackson@pa.org

CHATGPT HAS BROUGHT artificial intelligence into the mainstream, leading to predictions of everything from the end of work to the end of the world.

While these predictions lead to great headlines, the reality is that financial-services providers already use AI for things like chatbots and fraud detection. But as this technology advances, executives will be asked to make decisions about how to use AI throughout their businesses.

Since financial-services executives aren't technologists, they need to be prepared to ask good questions as they consider how to use AI. There are five areas of inquiry for internal teams as AI enters its next stage.

The first is, what is the technology being offered and how does it work? ChatGPT is just one kind of artificial intelligence that generates content based on using large datasets to predict what the most likely response to a question might be. Machine learning is another form of AI that uses algorithms to find patterns in data.

Understanding what kind of AI is being used, what data it needs, and what kinds of outputs it can deliver can help determine whether AI is a good fit for a particular company. The limitations of any possible AI tool also need to be considered. Does the tool create hallucinations, where AI delivers a false or even fabricated result?

A related question is whether AI is necessary. Does the company already have a statistical tool that does the same thing outside of a black box?

The second area of inquiry is, what does an organization need to do to use a tool? Is its data ready? Financial-services providers are often awash in data, but having a lot of data doesn't necessarily mean a company is ready to use AI. The data needs to be in a form that can be parsed by the tool.

Additionally, companies need to know how that data is managed, stored, and even used to create other products and services. The protection of data is a critical question going forward, which leads us to the third area of inquiry: what does a tool mean for privacy?

Because AI is trained on large data sets, researchers have found ways to pull data like names, phone numbers, and e-mail addresses from generative AI tools. Once financial-service providers put customer data into AI training sets, they need to ensure that data will not be leaked either publicly or to competitors if it is being fed to a third party that works with multiple banks.

This leads to the fourth area: what does artificial intelligence mean for fraud vulnerabilities and prevention? AI tools have been used to spoof people's voices to socially engineer fraud victims, and video is not far behind. In a presentation at the IPA's annual conference, Adwait Joshi, the founder of DataSeers, a company that applies AI to banking, said he sees a coming arms race as criminals and companies work to develop AI tools to attack, and defend against, each other.

The fifth area, which will be informed by all the other areas, is regulatory compliance. Federal banking regulators said in May last year that companies cannot hide behind algorithms to justify credit decisions. They must provide "specific and accurate explanations." This is why providers need to answer the preceding questions about what their AI tools do. We can expect more laws and regulations concerning privacy, fraud liability, and financial inclusion.

The next stage of AI in financial services has begun. The successful companies will not be the ones starting out with the most answers. They'll be the ones that ask the best questions. DT

TIME TO BE MORE THAN A PROCESSOR

Embedded financial solutions boost independent businesses and can make them clients for life.

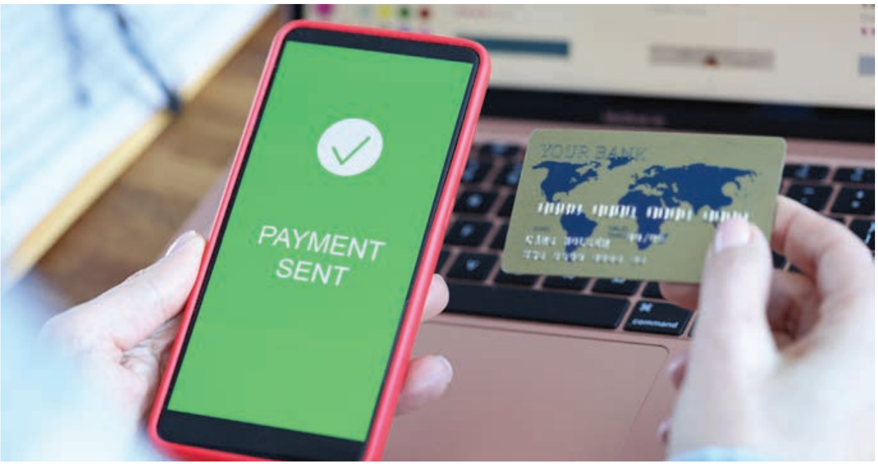
BY **JP CHAUVET**

JP Chauvet is the chief executive of Lightspeed Commerce.

THE FINANCIAL SERVICES industry is changing. While payment processors and traditional financial institutions will always have a place and purpose, they are no longer the only trusted options for financial services.

Embedded financial solutions—the integration of value-added financial services into software offerings—is set to redefine how consumers and businesses build and manage relationships. Non-financial companies, from tech and software-as-a-service companies to retailers, are diversifying their offerings to include financial solutions. Examples include omnichannel payment processing and lending, localized payment options, and cash advances.

When our company expanded into the embedded financial-solutions space, we wanted to bridge the gaps between merchants, consumers, and suppliers to create seamless payments technology for our customers. And in recent years, we added Lightspeed Capital to our financial offering to make funding accessible for independent businesses.



Embedded financial solutions present exciting opportunities to independent merchants. For these businesses, working with a company that offers a range of financial products supports business growth and success.

When it comes to financial services, customers are seeking holistic, direct experiences, according to a McKinsey report. Embedded financial solutions are addressing that need. They offer an integrated experience that combines the point of sale with payments and other financial products, reduce redundancies for independent businesses, and offer the flexibility to scale.

Businesses and their end customers benefit from these contextual, seamless experiences. Lightspeed can now unlock new use cases and often use proprietary customer data to improve financial access while reducing costs for end customers.

ONE-STOP PROVIDERS

Small businesses face systemic issues in payments. These include accessing, understanding, and using technology that can enable them to maximize their business potential.

Running a business can be time-consuming and complicated because these merchants are forced to rely on patchwork solutions. And if business owners don't have access to the right services, it can become costly.

Forward-thinking companies recognize that they can further empower their customers by offering embedded financial solutions to make key products and services available in one place for merchants. Payments and capital are and will continue to be two of the biggest offerings of embedded finance.

Using an all-in-one solution for every business need, from POS to payments, consolidates the entire experience and simplifies operations.

For example, an independent business working with a POS provider that doesn't offer embedded financial solutions will have to work with one or more third-party solutions. Now, let's say they're looking for funding to scale their store to a new location. That's another financial product they'll have to look elsewhere for—most likely a bank. Queue the lengthy application process, personal credit checks, and waiting period.

Managing a business this way can be exhausting. Instead, imagine how much easier it is to have the tools and technology you need at your fingertips with one provider. Businesses will be more likely to stay loyal to companies that can touch on different needs and deliver powerful solutions to their customers.

In working with one company, independent businesses get more value. They won't have to work with multiple providers to run their business. They will have access to valuable data, payments reporting, and accounting and analytics so they can find new ways to increase sales. All operations become streamlined, resulting in fewer errors as well as money and time saved.

Plus, one-stop providers deeply understand the businesses they work with. They have insight into business history, sales records, trends, and consumer data. This means merchants receive top-tier, personalized customer service.

One prominent example that captures the power of embedded finance is embedded payments. In our experience, seamless payment processing is at the top of the list of merchant requests. So we built an embedded-payments platform.

With embedded payments, your payment processor communicates with all of your sales channels from within your POS system to process transactions efficiently and without error. It's much easier for merchants to accept payments and consolidate crucial information in one convenient platform.

It's a massive time-saver. For example, there's no need to manually input transaction information, which greatly decreases errors and simplifies the sales process.

Capital is a powerful tool that businesses need to maximize growth and sales, but it isn't often easy to get. Small businesses traditionally have to go to banks or lenders to acquire funding. Lengthy applications, intense credit checks, and long waits are the norm.

As well, small businesses are often seen as less established, making it difficult for them to obtain funding. They can be limited by cash-flow requirements, their ability to put up collateral, and other factors that generally make funding from traditional institutions difficult to access.

That's where embedded financial solutions come in. A POS provider that also offers business funding or loans can give independent merchants a huge leg up, allowing them to invest in their business's growth.

REMOVING BARRIERS

A company with embedded financial solutions has greater insight into its merchants' businesses. Information on business history combined with data from POS and payment reports paints a comprehensive picture, giving companies the means to provide funding to a merchant based solely on metrics related to their business.

Large businesses with multiple store locations or a global footprint can benefit from embedded financial solutions as well. It's much easier to operate several stores when the POS provider and payment processor you use allows you to scale easily both online and offline.

For small and medium-sized businesses, embedded financial solutions remove many of the common barriers to success. It's not easy for these businesses to juggle patchwork solutions, which impede growth. Embedded financial solutions can help these owners reach their full potential. DT


Chauvet

Chauvet: "It's much easier to operate several stores when the POS provider and payment processor you use allows you to scale easily both online and offline."




HOW TO TAP REAL TIME'S POTENTIAL

With FedNow joining RTP in the race for real-time payments, a hugely practical service called request for payments could take off.

BY **STEVE MOTT**

Steve Mott is a payments consultant is a board director of the Faster Payments Council.

IF YOU'RE NOT a payments geek, you could be forgiven for wondering what all the fuss was about when the Federal Reserve announced in July that its real-time payments network, FedNow, had opened for business. If you are a payments geek, you cannot be forgiven for not realizing how FedNow might have changed the payments world forever.

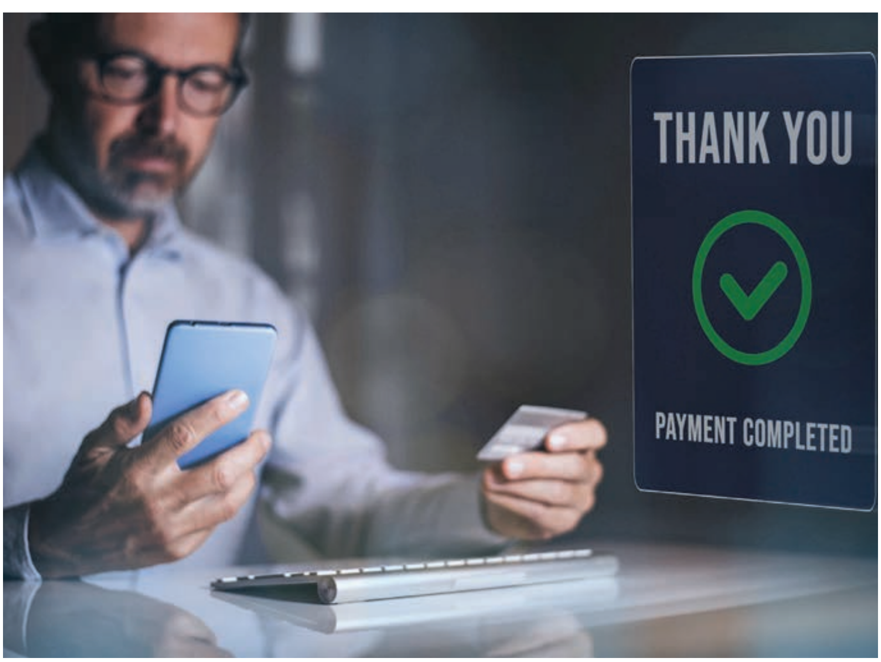
Here's why.

According to the Faster Payments Council, there are an estimated 150 faster-payment use-case development projects under way with banks, merchants, corporates, and third-party providers. They're crafting real-time payment solutions for long-festering but unaddressed problems involving paper checks, wires, cards, and even electronic checks.

When brought fully to market, the digital transformation of these slow, outmoded, and expensive forms of payment could generate tens of billions of dollars a year in savings for users and providers. On top of that, real-time payments promise to be much safer. What's not to like?

The problem is, until FedNow turned on its lights in July, all that promise and potential looked slated to take a long, slow, and deliberate path to market reality. That's because FedNow's main competitor, the Clearing House (TCH)'s Real-time Payment (RTP) system, has taken a more deliberate approach to what needs to be changed in payments and how quickly those changes need to take place, restricting use cases that can be addressed with its new, highly flexible and adaptable Request for Payment (RfP) mode.

But when FedNow opened its doors July 20, no such restrictions for its RfP mode were apparent. And



that means game on for payments innovation after all.

HOW RFP WORKS

So, just what is RfP? Well, most real-time payment systems use a payment mode called credit-push, where payment is made in a transfer from one user's bank account to that of another, including to and through another network, such as a card network. Today, there are six prominent providers of credit-push real-time payments—which are now a part of the U.S. payments landscape: TCH RTP, Visa Direct, Mastercard Send, Venmo, Zelle, and, of course, FedNow.

Credit-push is hardly an innovation. It has existed in the ACH network for a decade, and at TCH since 2017. But it is proving handy and efficient for the mostly business customers who use it. RfP, on the other hand, is new, and harbors radical potential for streamlining almost unlimited ways to pay—especially with consumer users.

RfP's flexible design can accommodate a host of applications, from earnest money deposits on mortgage loans to funding online-gaming accounts to point-of-sale payments (more on that later).

How does RfP work? The user agrees (typically on a biller's Web site, but also at the physical point of sale, with the service accessed through a URL-bearing QR code) to be billed for payment of an agreed-upon value and designates the bank account to be billed.

The billing entity (typically a corporation, or government entity, or even a merchant) then submits an RfP to its bank, noting the user's bank, identification, and amount. Those two banks then complete the payment transaction, which is settled on the RTP or FedNow network.

Current RfP protocols involve a series of messaging and processing steps more extensive than, say, those for card or ACH payments. But a crop of innovators has already emerged with ways to optimize these exchanges and minimize the time it takes to complete them.

So funding can be virtually instantaneous, and user recourse is highly limited, meaning good funds are indeed consummated in real-time, every day, 24 hours a day. An RfP transaction on TCH's RTP network today encompasses a round-trip, incurring a network cost of about a dime. Today, on FedNow, that RfP costs just a penny. Hence, all the excitement.

If, as executives of both networks have stated at various times, "we will take any payments our banks want to process," RfP stands to become a huge resource for payments innovation, filling new use cases, such as title and escrow payments, that are still laboring with paper checks and wires after decades.

That message hasn't been lost on most users of today's payment types. These include corporate customers looking to take advantage of digital technology with electronic wallets moving funds from bank account-to-bank-account (A2A). Or big retail merchants, who are looking to move beyond ACH for scalable A2A alternatives to card payments.

A CONSERVATIVE APPROACH

But TCH and FedNow have taken very different approaches to RfP's emerging role as a "Trojan Horse" of innovation.

TCH has been experimenting with RfP for more than a year, finally announcing Aug. 2 that it was officially supporting RfP—albeit with just a few conservative use-cases—owing to the network's concern over potential fraud risks and how to allocate the associated liabilities.

Quoting from TCH's announcement, the initial use cases are:

- **Consumer Bill Pay:** "Companies that provide recurring consumer services, such as utilities, can use RfP to request payment for their services;"
- **Business to Business Payments:**
  - Businesses can pay suppliers, business partners, contractors, freelancers or other third parties using RfP;"
  - Payroll providers can send RfPs to [their] corporate customers so they can fund payroll on the same day that employees are paid, rather than 2-4 days prior to payday;"
- **Account to Account (A2A):** "RfPs can be used by individuals to request transfers between bank or brokerage accounts that are owned by the same person. For example, brokers can send an RfP to customers so they can transfer money from their bank account to their brokerage account instantly to enable immediate trading."

Of particular concern to some of the biggest banks at TCH (which is owned by nearly two dozen of the largest financial institutions in the country) is the potential for fraud emanating from the very digital-wallet providers and A2A schemes corporate and retail customers are seeking to use.


Mott

Mott: "Request for Payment (RfP) debuts in a payments industry that has sorely needed better ways to pay."

Indeed, according to some participants on TCH's governing committees deliberating in recent months over this issue, some of the big bank owners were not ready to entertain any other options than funding of brokerage accounts.

These big banks were okay with digital-wallet offerings by regulated financial institutions (including PayPal, which processes Venmo transactions through RTP via Chase). But they reportedly rejected RfP use-cases for retail POS payments (i.e., those competing with cards) and possible use by non-regulated, non-bank networks (e.g., Apple/ Goldman Sachs).

On the borderline, but under observation, were wallet and A2A innovations in some morally sensitive areas such as online gaming (and even cannabis).

TCH appears to be toeing a careful line with these fast-growing (and potentially massive) new payments markets. Starting small with RfP and seeing what happens appears to be the current TCH strategy:

"As market adoption grows and RTP participants, billers, and payers gain experience with RfP, the permitted use cases on the RTP network are expected to expand to encompass all types of traditional and digital payment experiences. Learnings from these early adopters will be critical to that expansion and wide-scale adoption of RFP," the network said in its announcement.

FEDNOW'S CHANCE

That conservative approach leaves FedNow with an opportunity to run down the wide-open field with an expanded set of RfP use cases—if and when its initial cadre of participating banks chooses to support them.

RfP capabilities were available at FedNow's launch. And a number of banks and service providers are indeed scurrying to develop new applications and solve new use cases with the new network's RfP protocol.

It remains to be seen what the ultimate pricing will be to users, as banks and service providers will no doubt mark up real-time payment offerings at both networks. According to several corporate users, current RTP offerings are generally priced at three to five times ACH rates—for example, 75 cents to $1.00 for real time, versus 20 cents to 25 cents for ACH. And FedNow will no doubt be very sensitive to its own banks' concerns about security and liabilities.

Moreover, the Fed has consistently maintained for many months that it's open to what its banks want to do in terms of innovations, explicitly calling out the potential for POS use-cases—when its banks have tooled up for RfP and are ready to cater to corporates and retailers.

For their part, big retailers say they will come on board FedNow when its participating banks provide enough coverage, and when RfP solutions can handle the essential area of handling product returns and refunds. So the jury is still out on how quickly real-time payments will actually impact current payment streams.

Nonetheless, the clear contrast in the philosophies of these two key networks on the pace for accommodating and supporting payment innovation in the wake of relentless pressures to digitize the transaction economy offers the clearest choice yet for enlightened competition.

Such competition was the promise when—against big-bank arguments that the United States didn't need two real-time payment systems—the Fed decided the market needed FedNow after all. So Request for Payment (RfP) debuts in a payments industry that has sorely needed better ways to pay.

Learn About the Expanding Role of ATMs in the Evolving US Payments Landscape

NAC2023

ATMs ☆ ACROSS ☆ AMERICA

- Mandatory PCI Security Requirements - What You Need to Know to Keep Your ATMs Up & Running
- New VISA Program to Make Universal Deposit Taking Available at US Retail ATMs
- Federal Reserve Updates on CASH & a Potential US Digital Dollar
- And SO MUCH MORE!

October 24-26, 2023
Planet Hollywood Las Vegas Resort & Casino

Representing - Protecting - Serving
NATIONAL ATM COUNCIL
U.S. Independent ATM Operators®

GENMEGA
SWITCH COMMERCE
HYOSUNG INNOVUE
DNS DIGITAL NETWORK SOLUTIONS
Division of NCR KAHUNA ATM Solutions
Division of NCR Columbus DATA + SERVICES
NextATM
OptConnect MANAGED WIRELESS SOLUTIONS
CORD Financial Services
dpl Cash Management Services Powered by U.S. Bank
SMART
Triton
atmgurus PARTS · REPAIRS · TRAINING
ATMPartMart.com
SWITCH ALWAYS ON
LOOMIS
STAR FINANCIAL SERVICES
BELL ATM SERVICES WE KEEP CASH FLOWING
PARAMOUNT MANAGEMENT GROUP
cash2bitcoin
MBA USA LOCKS · TOOLS · TRAINING
ATM Geeks
PAI
Zem Media Digital Signage Solutions
MORPHIS
escarGOt Swift Mobile Chargers
ATM UP
NATIONAL ATM BROKERAGE
BLUWAV media.com
Coinwrap
PRO-SOLV SOLUTIONS
WTI WIRELESS

REGISTER NOW!

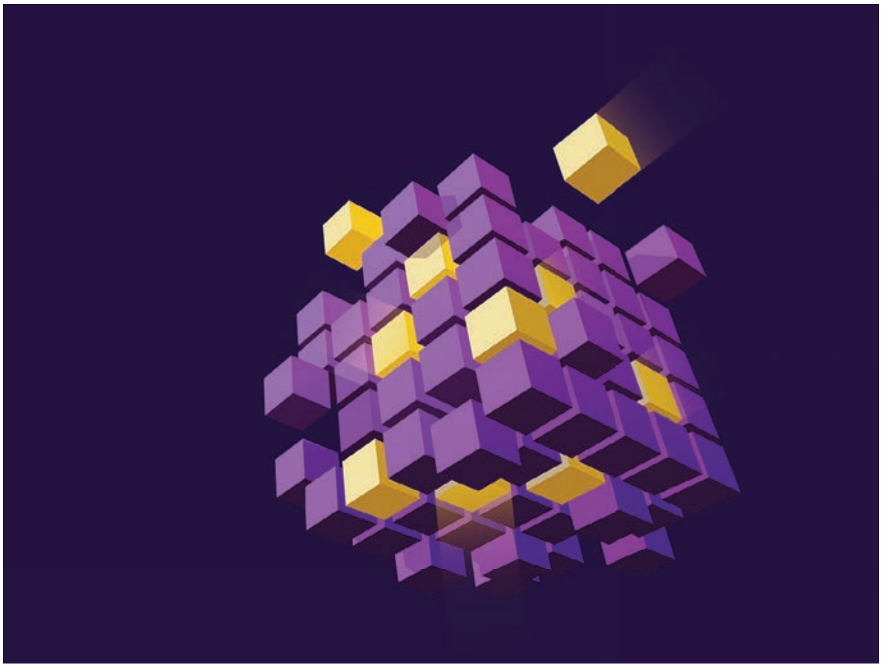
www.natmc.org

FOUR SHORTCOMINGS OF B2B PAYMENT TECHNOLOGY

Current technology is no longer as effective as it needs to be. Time to start adopting modern methods—including blockchain.

BY **MIKE SEKITS**

Mike Sekits is a co-founder and managing director of Btech Consortium and Strandview Capital.



IN 2021, business-to-business payments-market revenue was valued at $903 billion and is projected to reach $1.618 trillion by 2028. While these payments are an important service provided by community banks, existing B2B payments technology is not keeping up with customer expectations and innovation from fintechs.

This is due to the many challenges associated with B2B payments: cost, speed, security, flexibility, conditional payment triggers dependent on the delivery of goods, and the ability to match the paperwork.

To start, B2B payments tend to be larger than consumer payments and often require supporting documents before a payment can be made, such as a payment order, invoice, and proof of delivery. As a result, additional scrutiny is necessary when comparing documents and amounts. Customers challenge the costs when the amounts do not match the payor/recipient's expectations. Adding to the paperwork, 40% of B2B payments are still made through paper checks.

For community banks, a failure to streamline the payment process can lead to mistakes, delays, and more costs. But how can the process be improved when the solutions provided by traditional core-technology providers servicing community banks fall short?

Resolving B2B payments challenges is one of the leading reasons why community bank-driven venture-capital groups are pooling their resources to fund the technology development needed to address the issue.

Here's a rundown on the common issues with current B2B payment processes:

PAYMENT DELAYS

The most common challenge for B2B payments is timing delays, often due to mail slowdowns and mistakes in the manual-entry process when sending or receiving checks.

As a result of these problems, a bank's client may be late in making its payments, requiring notice, potential late fees, and sometimes a service halt. This type of friction in the process can be incredibly frustrating for banks' customers and their clients and can detract from the value banks are supposed to provide.

In the interim, banks can help businesses mitigate this risk and hassle by ensuring clients know exactly how much they will be billed and, when possible, using electronic invoicing processes. Businesses can automate the delivery of invoices to clients and ensure they receive the correct documentation immediately. Often, this can be achieved by integrating accounting software with community banks' bill-payment services.

PAYMENT METHODS

Sometimes, the method by which payments are made or received can also create significant problems. For instance, if a business client pays by check or money order, it can take additional time for the payment to be cleared, adding to an already lengthy process. Also, payments platforms might not allow a business to accept the preferred payment method used by its clients.

For the time being, banks that offer embedded, electronic payment solutions and adopt mobile-payment options can mitigate this issue.

MISCOMMUNICATION AND ISOLATION

B2B payments involve multiple internal and external teams to handle several processes before the payment can be made. As a result, a lack of external or internal communication can impact a payment's timing and success. Also, miscommunication between the two parties can make things fall through at the last minute, resulting in delays and potentially impacting a business's bottom line.

PROBLEMS WITH SECURITY

B2B payments represent a massive volume of data, as well as large transaction amounts, compared to the consumer segment. Thus, security is a major concern for B2B customers, as they have their own and their customers' data to protect and are subject to greater liability in the event of a security breach.

With the proliferation of data breaches in recent years, businesses are more mindful of protecting their data on all fronts, and bank-account data is some of the most sensitive out there. Therefore, the bank is responsible for guaranteeing its security through the processes and checkpoints it adopts as part of the payment process.

Blockchain, though still in the early stages of adoption, can provide a highly secure network to store transaction data along with payments through distributed ledger technology. The information sent through blockchain is encrypted, making it more difficult for outside parties to gain access.

Inherently, blockchain technology limits the amount of information obtained in a breach, making it harder to obtain large amounts of data with one hack. It also provides a more transparent record of data, helping to ensure nothing is changed without proper notification and creating a consistent source of truth and accuracy that other databases struggle to maintain.

SOLUTIONS ON THE HORIZON

In the next few years, we expect most payments to move into the FedNow real-time payments program or onto new technology rails provided by fintech vendors, including private-permission digital ledgers, blockchain, or stablecoin platforms.

The better news is that B2B payment platforms have recently been developed at a fraction of the cost and time big banks are spending to develop the technology internally. Community banks can catch up by evaluating and adopting newer platforms and integrating them into their customers' accounting/ERP solutions.

We also see adoption of more payment-management platforms, which serve as a central hub for all processes to increase visibility. This allows everyone to see who is responsible for what tasks, what conditions need to be met before payment, when payments are due, and the terms of such payment.

Ultimately, alignment between all parties is the key to a streamlined B2B payment process, and using a common payment platform is the best way to ensure this happens. Private, permissioned ledgers using blockchain technologies can provide these types of payment platforms. Examples of young but proven companies that deliver innovative B2B payment solutions and payment platforms are Tassat and Figure.

As business customers continue to shift toward digital solutions versus manual processes for banking, community banks must invest in solutions to meet their customers' needs while considering the current issues holding them back.

Technology companies are rapidly building applications for smaller banks, and technology consortiums are being formed specifically to aggregate the resources for community banks. The result is that B2B payment technologies—including blockchain applications—are being developed in trade finance, mortgage warehouse lending, securitization trusts, loan servicing, and logistics business sectors. DT


Sekits

Sekits: "In the next few years, we expect most payments to move into the FedNow real-time payments program or onto new technology rails provided by fintech vendors."

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 Publisher Bob Jenisch today:

877-658-0418
bob@digitaltransactions.net

WHO WILL ROUTE TRANSACTIONS?

The Credit Card Competition Act is back in play. But as Congress debates the bill, a pressing question looms about its biggest requirement: Who are the Visa and Mastercard alternatives supposed to be?

BY PETER LUCAS

Senator Richard Durbin is back at it. After failing to advance the Credit Card Competition Act out of Congress last year, the Illinois Democrat has reintroduced the legislation in the new Congress. Not only is the bill generating more buzz, it enjoys more bipartisan support in both chambers.

The bill is the latest salvo in Durbin's long-running battle to break Visa's and Mastercard's grip on the credit and debit card business. Boiled down, it says if Visa is one of the network choices offered by issuers to merchants, the other choice can't be Mastercard, and vice versa.

If passed, the CCCA would apply to financial institutions with $100 billion or more in assets. These are generally the largest card issuers, controlling better than 90% of the credit card market.

U.S. merchants' fees for credit card acceptance exceeded $90 billion in 2022, making the U.S. one of the most expensive card markets in the world, according to the Atlanta-based consulting and research firm CMS Payments Intelligence Inc.

As expected, large banks, Visa, Mastercard, and bank trade associations are lobbying hard against the bill, while merchants and their respective trade groups are pushing for passage. The latest argument against the bill is that it would strip issuers of the funds needed to support rewards and other cardholder benefits, since competing networks could charge lower merchant fees. Merchant groups and other proponents of the bill say otherwise.

All this political back and forth over the CCCA is to be expected. But a huge unanswered question looms: Which networks would compete with Visa and Mastercard to route credit card transactions?

'POLITICAL CONCERNS'

The choices that immediately jump to mind are American Express, Diners Club International, Discover, and the regional debit networks. The latter are the most intriguing and, some say, controversial options, as the prevailing belief among payments experts is debit networks would compete for credit card traffic if the CCCA passes.

But the debit networks, some of which are controlled by the nation's largest transaction processors, aren't talking about their plans should the CCCA become law. The frequent response is that they are evaluating their capabilities to route credit card transactions.

Fiserv Inc., which owns the Star and Accel networks, said just that: "We are evaluating our technical capabilities which could support the requirements envisioned by the Credit Card Competition Act," a Fiserv spokesperson told Digital Transactions by email. "This includes the ability for single-message debit networks that can route PINless transactions, such as STAR and Accel, to pursue the credit market for the first time."

While such a response sounds vague, payments experts argue that at least some debit networks would be happy to jump into the fray. But for now they're keeping a low profile as the CCCA works its way toward a vote. The reason? They fear they may face a backlash from Visa and Mastercard and their bank customers.

"The skittishness on the debit networks' part isn't over business concerns, it is over political concerns," says Doug Kantor, an executive committee member of the Merchants Payments Coalition and general counsel for the National Association of Convenience Stores.

"The debit networks have the capacity to fill this role," he adds. "especially since credit card volume will not all flow through one alternative network and the decision on which alternative networks to support will be made on a bank-by-bank basis should the CCCA pass. But the banking industry has worked itself into a frenzy over this issue."

Indeed, the politics surrounding "this issue" are so messy that Durbin's office and that of Sen. Roger Marshall (R-Kansas), a CCCA co-sponsor, did not respond to inquiries from Digital Transactions about which networks could serve as alternatives to Visa and Mastercard should the CCCA pass.

Politics aside, one debit network executive who spoke on condition of anonymity says a big reason the debit networks are not tipping their hand is that, until the legislation passes, there are no concrete rules governing network choice or how the law will be enforced.

"As of now, we have no plans to move into credit card processing as we don't know how it will play out if the CCCA passes," the executive says. "If our bank customers want to move in that direction, we'd pursue it because we work for them."

CO-BRANDING, ANYONE?

Payment experts also caution that uncertainty surrounds how the industry as a whole would respond to passage of the CCCA, simply because of the rapidly changing payments landscape. "Who knows what payments will look like in five to 10 years," the debit network executive says. "This is a complicated business and uncertainties exist around this issue."

If the debit networks—which also include major systems like NYCE (owned by processing giant FIS Inc.), Pulse, and Shazam—are not inclined to be alternatives to Visa and Mastercard, then who is?

American Express, Discover, and even Diners Club (owned by Discover), are frequently mentioned choices. The prevailing belief among experts contacted for this story is that these three networks would be unlikely to charge cut-rate merchant-processing fees for general credit card processing. That would help protect card-issuer margins but frustrate merchants.

"If a card issuer has to offer the choice of an alternative network, [it] won't pick one that obliterates [its] pricing structure, [it is] more likely to pick one with a like pricing structure," says David Shipper, a strRileyategic advisor for Datos Insights, which was formed in June after the merger of the consulting firms Aite- Novarica Group and RBR. "The debit networks have a history of bringing down interchange fees, so [issuers] are likely to prefer AmEx and Discover."

Because card issuers would be required under the CCCA to include the logos of networks they support on their cards, that stipulation may lead to opportunities for AmEx and Discover to enter into co-branding agreements with issuers.

That scenario could keep those networks from undercutting Visa and Mastercard since they would have a stake in the interchange earned on a cobranded card transaction processed through their respective networks. Such a scenario can be a dealmaker, but may not please merchants.

"If an issuer puts a Discover bug on a card as an alternative network choice, it can open the door to

Mott: "A lot of [network] players won't be looking to be the first to jump off the diving board."

co-branding opportunities," says Brian Riley, co-head of payments at Javelin Strategy & Research. "A bank needs a partner as an alternative network."

SO LONG, REWARDS?

While offering a lower price can quickly net debit networks lots of credit card volume should the CCCA pass, there are risks involved in that strategy.

"Competing on price can be effective initially, but over time you need a margin to service the operation, otherwise processing becomes a loss leader, and when that realization hits, that's the wakeup call when a processor starts thinking, 'is this a good business model,'" notes Riley.

Some experts also argue that lower transaction costs for merchants through network choice could hurt issuers' ability to dip deeper into the risk pool when offering cards to consumers.

As interchange revenues decline, issuers may have to look for new ways to generate income to cover the shortfall, such as raising interest rates for high-risk cardholders, reducing credit limits, or cutting back on the number of potential new customers they target. In any of these scenarios, consumers would feel the effects of those moves.

"Inflation is still occurring, and if the economy tanks and issuers see lower margins, they will start to rethink where they take risk with consumers," Riley says. "Issuers know the processing pricing model affects income which goes to operations, collections, and customer service."

Another area where issuers might make up lost revenues from more competitive network pricing is in the business of cardholder rewards. That argument has been loudly trumpeted by the Electronic Payments Coalition, a trade group that represents banks in opposing the CCCA.

Research from CMSPI claims passage of the CCCA would have a minimal effect on card issuers' ability to continue funding credit card rewards. But in July, the EPC redoubled its argument that the bill would strip issuers of the funds needed to support rewards.

In its statements on the issue, the EPC argues that "historical evidence, demonstrated through myriad academic studies, shows that the proposed credit card routing mandates will likely lead to a drastic reduction of rewards programs."

For its part, CMSPI acknowledges that card issuers would see an average 37-basis-point reduction in interchange revenues on Visa and Mastercard transactions if the CCCA is passed. But consumers would incur, at most, a less than 0.10 percentage-point drop in rewards benefits, the research firm says. CMSPI's projections are based on data from Australia, where card swipe fees were capped at 0.8% in 2003.

"We estimate there is an average margin of 30% on interchange revenues net against rewards expenditures," says CMSPI chief economist Callum Godwin. "CMSPI estimates that merchants could save $15 billion annually from CCCA, which equates to a 16% reduction in fees."

"Given the size of the U.S. credit card market," Godwin adds, "there is a strong incentive for multiple parties—including domestic debit networks, global credit card networks, and possibly new solution providers—to participate as alternative network

Riley: "Issuers know the processing pricing model affects income which goes to operations, collections, and customer service."

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.

Shipper: "The debit networks have a history of bringing down interchange fees, so [issuers] are likely to prefer AmEx and Discover."

providers." In that scenario, those alternative networks will have to compete for issuers' favor.

A TIPPING POINT

The prospect that passage of the CCCA would attract new solution providers is an argument that is beginning to gain traction. The most likely new providers would be fintechs, which provide technology to payments providers to better manage their operations and processes.

"What constitutes a network is different today from what it has historically been," says Steve Mott, principal at payments consultancy BetterBuyDesign. "There comes a point in time where new networks come along that can say to banks, if card issuers want to control the economics around the Visa and Mastercard networks, they can."

When that tipping point is reached, Mott argues, large banks will begin to rethink Visa and Mastercard's one-size-fits-all network approach. Mott says he has had discussions with some large banks that are ready to begin exploring the idea of what more network competition would mean for their card business.

"The CCCA can open the door for banks to wait and see what happens when it comes to network competition," Mott says. "If true network choice is there, the technology is there for new players to boost competition. There are several large banks in a position to take steps to get intermediaries out of the revenue stream. The role of the network is to serve, not enslave."

If the CCCA passes, however, Mott does not see a wave of players charging out of the gate vying to launch new technologies as alternative networks. "It takes a lot of money to bankroll these types of initiatives," he says, "and for the first year or so, I think a lot of players won't be looking to be the first to jump off the diving board."

As with any legislation, a big question is what kind of teeth regulators will put behind enforcement of the CCCA. Payments executives note that even after passage of the Durbin Amendment to the Dodd-Frank Act in 2010, which capped debit card interchange, there was a lot of foot-dragging by the industry when it came to implementation, and additional rule-making and clarification was needed to plug holes.

One such clarification came from the Federal Reserve and took effect July 1. The Fed's move came in response to years of hesitation by banks on compliance with the Durbin Amendment's requirement that merchants have a choice of networks in debit card routing for e-commerce transactions, not just in-store sales.

"Debit routing rules haven't always worked so well," says Bob Steen, chairman of Mechanicsville, Iowa-based Bridge Community Bank, which is a member of the Des Moines, Iowa-based Shazam debit network. "Many small merchants don't know they have a routing choice."

Proponents are confident the bill will pass during the current session of Congress. If nothing else, passage could open the door to increased network competition that might potentially save merchants $15 billion a year in acceptance costs, according to CMSPI.

"If there is a path, the free market works," Steen says. "What the sponsors of the CCCA are saying is that the market should allow for competition." DT

MISCODED MERCHANTS CAN BE A SEVEN-FIGURE MISTAKE

Pay attention to your MCCs,or pay a hefty price later on.

BY ALAN PRIMITIVO AND WILL SEITZ

Alan Primitivo (left), is the vice president of client operations and Will Seitz is the regional director of sales at G2operations

MERCHANT CATEGORY CODES (MCCs) play a central role in payments risk management, but too many service providers and acquirers take them at face value. Now, in the wake of renewed focus on MCCs by the payment networks, miscategorized MCCs can be a very costly mistake.

Recently, our payments risk-management firm has seen the assessments levied against payments acquirers for miscoded MCCs reach upwards of seven digits.

Let's look at recent developments, key challenges, and some recommended actions for acquirers.

This summer, the Visa Integrity Risk Program (VIRP) entered the card-payments landscape, replacing the previous Global Brand Protection Program (GBPP). Risk-management programs by card companies are not new, but any time new standards are introduced, scrutiny is heightened. MCCs are getting extra attention right now, and acquirers that bear most of the risk must respond accordingly.

Under VIRP, "high integrity risk merchants" are now categorized into three tiers that are subject to assessments. High integrity risk merchants are business types that pose a greater risk of processing illicit transactions. In the new three-tier structure, tier 1 has the highest level of risk. Here are all three tiers as described by Visa:

Tier 1 merchants operate businesses "where there is a higher risk of illegal activity occurring without proper controls and that potential illegal activity could—either directly or by association—cause significant harm to the health, safety, and/or well-being of individuals." Tier 1 is specific to card-absent adult content, dating and escort services, gambling, and pharmacies.

Tier 2 merchants have a higher risk of illegal activity that could cause financial or other economic harm to individuals. Tier 2 business types include card-absent crypto merchants, digital file sharing, and games of skill.

Tier 3 merchants have "a higher risk for non-compliance with regulations or deceptive marketing practices without appropriate controls." Examples include outbound telemarketing, high-integrity-risk financial-trading platforms, and negative-option subscriptions.

THE COMPLICATED ENVIRONMENT

Categorizing merchants can seem

straightforward, but the reality is complicated and dynamic. Miscategorized merchants are often a much larger problem than most acquirers realize and, as a result, their portfolios carry more risk than is readily apparent. In our experience, nearly half of MCCs in the average merchant portfolio are either misclassified and should be assigned a more-specific category or are altogether missing.

The reasons for this are many—some innocuous. For example, many merchants that could fall under more than one MCC often land in a "miscellaneous" category. While the broader miscellaneous MCCs are sometimes appropriate, they can also become a catch-all with opaque levels of risk.

Another scenario occurs when the initial MCC is accurate but becomes less so over time as the merchant expands offerings beyond the code's original definition. For example, the risk profile of a restaurant changes when it begins selling alcohol.

Risk tolerance is unique to each payment-service provider, affecting both compliance risk and revenue. Legitimate, high-risk merchants can be highly desirable, as they generate more revenue. At the same time, seemingly low-risk merchants are not all safe from network fines and assessments.

And some MCC misclassifications are intentional. For example, a merchant may try to conceal riskier transactions to garner a more favorable rate with processors. More deceptively, a merchant may present a benign-looking shell business to hide transaction laundering. Gadget sites, for instance, are common front businesses for transaction launderers.

Another complicating factor, particularly for e-commerce, is jurisdiction. Operating an online business removes geographical barriers and opens the door to transact business and ship goods anywhere in the world. This poses problems for products with legality that differs across jurisdictions.

For example, cannabis laws vary widely from country to country—and even state to state within the United States. A cannabis merchant that ships products to another jurisdiction can easily run afoul of the law. That is why it is so important for acquirers to assign the most-accurate MCC for each merchant, as well as monitor every merchant for the life of the account.

ACTIONS TO TAKE NOW

MCCs are central to managing both risk and revenue. Fines for violating payment network requirements can be staggering, and are often tied to an infraction's length of time. That said, low-risk merchants don't ensure compliance, and high-risk merchants can generate significant revenue. To get the balance right:

1. **Define Your Risk Tolerance:** Clearly articulate what "acceptable risk" is for your organization. As part of this process, create your own list of approved MCCs, which helps establish a framework for merchant selection. Regularly review and update the list to keep pace with business conditions and regulatory changes.
2. **Scrub Your Portfolio:** Each missing or inaccurate MCC code represents increased risk and the potential for lost revenue. Make it a priority to review each merchant's offerings and assign the most-accurate MCC code.
3. **Monitor for Changes:** As merchants grow their businesses, they add and remove products and services, which can change their risk and revenue profile. Regular monitoring is critical for reducing the risk of network assessments while still meeting revenue targets.

Especially now, it doesn't pay to leave the accuracy of MCCs to chance. Content violations can be sudden, unexpected, or may lurk indefinitely without oversight. Ultimately, even absent the risk of fines, accurate MCCs are a valuable tool for managing risk and growth. Acting now will provide a clearer picture of risk—and improve portfolio profitability. 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**