DIGITAL TRANSACTIONS®
Trends in the Electronic Exchange of Value

AI TAKES TO THE FRAUD PREVENTION FIGHT

Criminals' increasing adoption of AI to power fraud schemes is leaving merchants and payment providers little choice but to fight back–with AI.

Volume Twenty-two, Number Four • DigitalTransactions.net • April 2025

ALSO IN THIS ISSUE:

celero

FUSION

Focus on building and selling exceptional software

Let **Celero Fusion** simplify and streamline payment processing for you.

Explore our tailored solutions, quick implementation, and dedicated support team

contents

APRIL 2025 • VOLUME 22, NUMBER 4

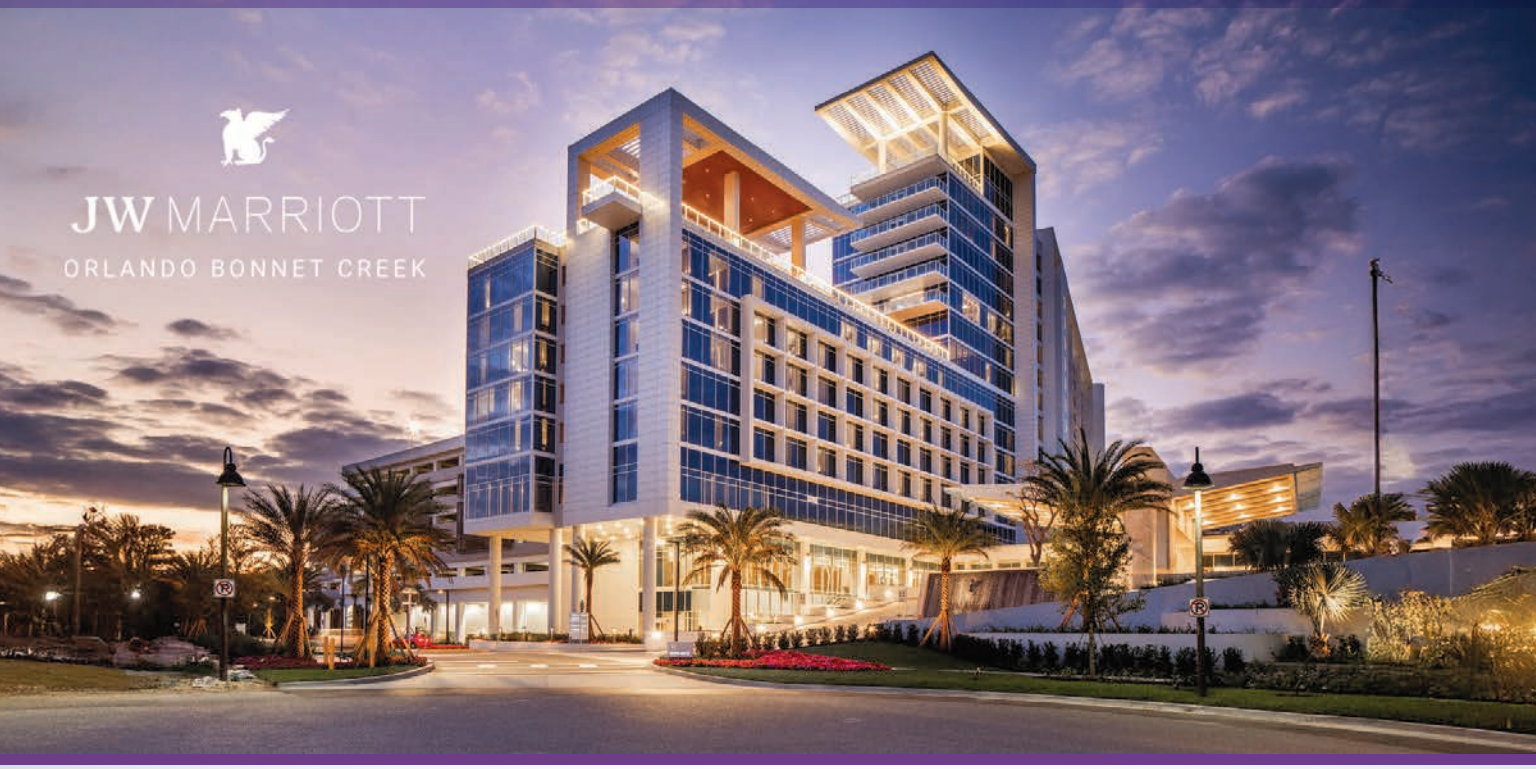
AI Takes To The Fraud Prevention Fight 22

Criminals' increasing adopion of artificial intelligence to power fraud schemes is leaving merchants and payment providers little choice but to adopt the technology to fight back.

Cover Photo: Adobe Stock generated with 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.

JOIN US IN ORLANDO • JUNE 2 - 4



ORLANDO

SEAA 2025

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

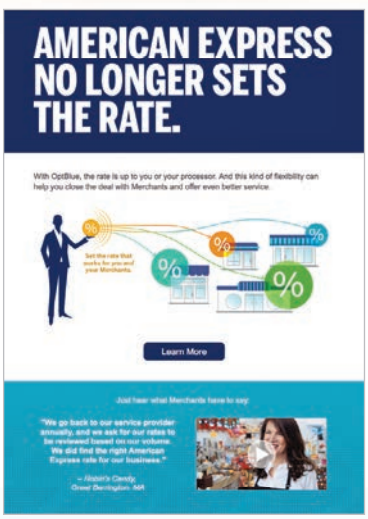
Register now for a truly rewarding event that brings payments industry leaders together to help equip agents and sales offices with the knowledge and tools to be more successful. SEAA 2025 is the perfect time for you to network with payments industry leaders, get a first-hand look at the newest technology and grow your business with the latest product offerings. But spaces for exhibitors are filling fast - visit us online to reserve your spot now!

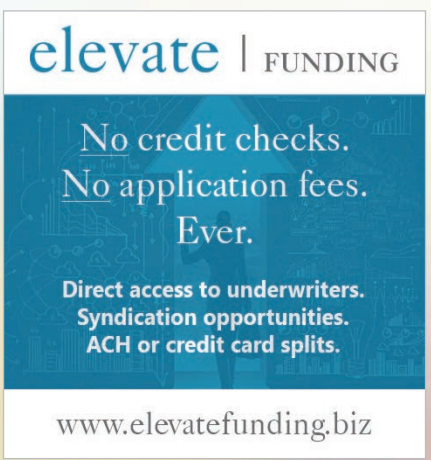
FOR REGISTRATION, AGENDA AND UPDATES

WWW.SOUTHEASTACQUIRERS.COM

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

the gimlet eye

HAS THE TIME COME FOR STABLECOINS?

THE ANSWER TO our titular question may be yes, and sooner than you think.

A leading merchant association and a group representing stablecoin interests have thrown their weight behind efforts to bring stablecoins into the U.S. payments mainstream. The move by the Merchant Payments Coalition and the Payment Choice Coalition seeks to "promote their shared goals of enhancing innovation, competition, and choice in U.S. payments," the two groups said in a statement released last month.

The MPC argues stablecoins—cryptocurrency whose value is tied to a fiat currency such as the U.S. dollar—would represent an innovative approach to making retail payments more efficient. Indeed, stablecoins "represent a much less expensive proposition for merchants on a per-transaction basis," Aaron McPherson, principal at AFM Consulting, told us.

But estimates of acceptance costs for digital currencies like stablecoins vary, while spotty retail acceptance makes it hard to arrive at associated costs. "The cost to establish acceptance of stablecoins may be a barrier for some merchants, because they would have to integrate wallets into their existing checkout systems, but today's technology stack should make that easier," figures McPherson.

Experts like McPherson say the latest move by the MPC and the PCC shouldn't be underestimated, as it is "both a big step forward for stablecoins and a way to bring down the cost of acceptance compared to credit cards," he notes. The MPC says it is backing legislation "to provide a solid, reliable regulatory structure for stablecoins" while the PCC is looking "to ensure a competitive payments landscape," according to the joint statement from the two groups.

Merchant groups have long decried the cost of card acceptance. The MPC along with other merchant groups has backed the Credit Card Competition Act, legislation aimed at moderating credit card acceptance costs by requiring processors to offer a choice of networks. The PCC represents small businesses and trade associations, as well as companies involved in working toward regulation of stablecoins.

So could this type of crypto find a foothold where digital currencies like Bitcoin haven't? The maddening answer is a great big "maybe." Stablecoins, like other digital currencies, remain a fringe payment method, though their very stability of value sets them apart in contrast to the often wild swings in value holders of coins such as Bitcoin have experienced.

Still, it remains unclear for the time being how many merchants would be willing to accept the coins. That's critical. "Merchant acceptance of stablecoins is absolutely crucial for them to get traction in the U.S.," notes McPherson. However, they could catch on sooner with the general public, he notes, adding, "they are already popular in African countries."

John Stewart, Editor | john@digitaltransactions.net

APRIL 2025 • VOL. 22, NO. 4

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.

BPA WORLDWIDE

Talk to Us
About Our
Personalized Services

At **Merrick Bank**, 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 deliver solutions designed around you!

Contact us today to set up an appointment.

merrickbankacquiring.com/contact

Merrick Bank®
Merchant Acquiring

DIGITAL WALLETS WIN IN THE SENATE—NOW WHAT?

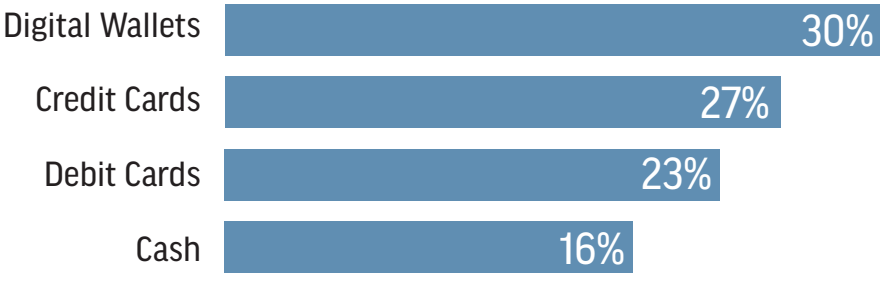
The U.S. Senate early last month voted 51-47 to scrub a regulation issued in November by the Consumer Financial Protection Bureau and aimed at mobile wallets and digital money transfers. The repeal legislation, which moved to the House of Representatives, comes as major payment-app developers like Apple Inc., Block Inc., Google LLC, and PayPal Holdings Inc. faced new rules that would give the CFPB enforcement capability in an area where it has had only examination authority.

The legislation also comes as the arrival of the Trump Administration has led to sweeping changes in regulatory enforcement across the federal government. Trump on Feb. 1 fired CFPB director Rohit Chopra, under whose aegis the payment-app rule had been developed. Conservative political analyst Russell Vought took over as acting director a week later.

The Senate action, at least, is likely to encourage major developers of payment apps, observers say. "For fintechs, it is a victory. The pendulum is swinging in the other direction," says Scott Talbott, executive vice president at the Electronic Transactions Association, a Washington, D.C.-based trade group.

MOST USED PAYMENT METHODS WORLDWIDE

(Share of transaction value, 2023)



Source: Morning Consult

The 259-page payment-apps rule, which had been set to take effect 30 days after its publication in the Federal Register, applies to firms that process at least 50 million consumer transactions per year. Combined, the biggest firms covered by the regulation process more than 13 billion transactions annually, according to the CFPB's estimates. The new regulation would also have added enforcement capability to the CFPB's remit in this area, where before its actions were limited to examinations.

Areas of supervision under the rule include privacy and surveillance, errors and fraud, and so-called debanking, or the interruptions consumers may sustain when app service is temporarily lost without notice. "Consumers have reported concerns to the CFPB about disruptions to their lives due to closures or freezes," the CFPB noted in a release issued in November.

Consumer advocates have deplored the Senate's action, charging that consumers will be at higher risk of fraud and disclosure of sensitive financial data. "Repealing the CFPB's rule is major win for big tech that leaves consumers vulnerable to losing money

to payment app fraud and puts the privacy of their sensitive financial data at risk," said Chuck Bell, advocacy program director at Consumer Reports, in a statement. "We need to preserve the CFPB's authority to conduct regular examinations of digital payment-app providers to make sure they are following the law and to protect consumers from unfair practices before they become widespread."

By mid-March, it was hard to tell how the legislation would fare in the House, though the Senate vote unfolded almost entirely along party lines, with Democrats against and Republicans for, with the exception of Josh Hawley, Republican from Missouri. "This says Big Tech has had some success in repairing relations with Republicans," notes Eric Grover, proprietor of the consultancy Intrepid Ventures. "We'll see what happens."

— John Stewart

TAP-TO-PHONE IS BOOMING FOR VISA

A 3-year-old technology enabling merchants to accept contactless payments using a regular smart phone with no special hardware has scored a global year-over-year growth rate of 200%. That rate is even higher in the United States, United Kingdom, and Brazil, the three countries with the highest adoption rates, Visa Inc. said in March.

The growth rate in these three markets is 234% on the VisaNet system. Visa did not release actual usage data. Visa announced the Tap to Phone technology in 2020. Versions of it are available for Android and Apple smart phones. Apple's service launched in 2022. For its own offering, Google uses the name Tap to Pay on Android.

One advantage of the technology is that no external device is needed to accept payments. The NFC chip in contactless cards is able to communicate with the NFC chip in many smart phones, using dedicated software to secure and process the transactions. This process is often called softPOS because it eschews dedicated POS hardware.

This option is especially popular with small businesses, which account for nearly 30% of all Tap to Phone merchants, Visa says. Adoption is particularly high among beauty and barbershop operators, restaurants, and retailers.

One of the drivers of the growth is that the technology is suited for merchants of any size, Visa says. "Tap to Phone is a tech equalizer that allows sellers of all sizes, including new small businesses and micro-sellers, to access the same digital payment tools as large retailers," Visa said in a statement to *Digital Transactions*.

Other factors are expanding support from processors and acquirers and the increasing confidence small businesses have in digital payments. Visa says new use cases have helped—such as Tap to App Card, which enables users to add eligible credit and debit cards to digital wallets with a tap; Tap to Confirm to authenticate a high-value transfer; and Tap to Send and Request money, which enables tapping a card to a device wallet to send funds.

"The shift toward digital payments, particularly in cash-dominant markets, is driving the growth of Tap to Phone as businesses transition from cash-only to secure digital payments," Visa says.

— Kevin Woodward

Visa CEO Ryan McInerney: Visa tap to phone is live in 118 markets worldwide.

COINBASE APPEARS TO BE OFF THE HOOK

A top executive at Coinbase Global Inc. indicated in late February the Securities and Exchange Commission had withdrawn an enforcement action against the cryptocurrency platform, a move the executive lauded as a "victory not just for Coinbase, but for our customers, the United States, and individual freedom."

"We've always maintained that we were right on the facts and the law, and today's announcement confirms that this case should never have been filed in the first place," said Paul Grewal, chief legal officer for the San Francisco-based company, in a blog post. Officials at the SEC did not respond to a request for comment on the matter.

The regulator sued Coinbase in June 2023, alleging it was operating as an unregulated broker. In January, Mark Uyeda took over as acting chairman of the agency as the incoming Trump administration began replacing the heads of various arms of the federal government. Activist head Gary Gensler resigned Jan. 20 after three-and-a-half years as chairman.

Grewal in his post characterizes the SEC as a "rogue regulator" and called the news "a clear vindication of our position." He also contends Washington needs to go farther in buttressing the position of digital-currency firms. "It is critical that we pass legislation which provides the long-term certainty needed for the U.S. to lead in this industry," he notes. Founded in 2012, Coinbase operates a cryptocurrency exchange that allows users to buy and sell digital currencies, as well as store them.

Experts who follow the developing crypto market lauded the SEC's withdrawal of its litigation against Coinbase. "It's a good thing," says Aaron McPherson, founder and principle at AFM Consulting Inc. "This regulatory overhang has been creating a lot of uncertainty and reluctance to invest [in crypto firms. Coinbase has proven stability and is well run. You wonder if the FTC under Gary Gensler didn't think a cryptocurrency exchange should exist."

But McPherson is careful to distinguish between established companies like Coinbase and other firms whose foundations may be less solid. "I never thought shutting down Coinbase was the answer, but there has to be a separate regulatory regime for cryptocurrency," he argues. "A lot of crypto offerings are immature, [which] makes it much riskier for investors, so there does need to be some thinking about what kind of protection needs to be in place." One such area that stands out, he says, concerns information for users and investors. "There needs to be even more disclosure," he argues.

The picture may now brighten, not just for Coinbase but for other crypto firms, McPherson contends. The SEC's latest action is "a good thing," he says. "This regulatory overhang has been creating a lot of uncertainty and reluctance to invest."

Investment aside, spending may be on the upswing, as well. Just since the inauguration of Donald Trump, whose administration has been seen as more favorable toward digital currency than its predecessor, the volume of crypto spending has shot up 36% compared to the same period a year ago, according to BitPay Inc., a cryptocurrency platform.

— John Stewart

MONTHLY MERCHANT METRIC

Account Attrition

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

	Account Attrition %	Volume Gross Attrition %	Net Revenue Gross Attrition %
Jan'25 (T3M)	-21.7%	-13.2%	-18.5%

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

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

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

PAYSAFE'S TOP BRASS BRUSHES OFF TAKEOVER RUMORS

By early March, rumors about an acquisition of Paysafe Ltd. had swirled around the company for nearly a month , and the processor's top management were in no hurry to add fuel to the speculation.

"We're going to stick to no real comment," said chief executive Bruce Lowthers while addressing an equity analyst's query about the matter. "We've had inquiries come in. We feel we're creating a lot of value, so it was not unexpected." Ultimately, he said, the Paysafe board will decide the matter.

Speculation about a takeover briefly drove Paysafe's stock to nearly $24 per share on Feb. 6, but that momentum quickly drained and the shares soon settled into high-teens territory over the ensuing days. The stock closed on March 14 at $15.81.

With the passage of time since the rumors emerged, some observers have concluded the company may simply have put the matter on the shelf. "It could be they were just testing the economic winds, favorable or foul," notes Cliff Gray, proprietor of Gray Consulting, in an email message to *Digital Transactions*.

Testing the market or not, Paysafe has some reason to boast. "We have proven our ability to accelerate growth," Lowthers said during an earnings call early last month. "I'm more optimistic [for the company] today than I was three years ago when I joined Paysafe." He cited "solid growth" in the company's small-and-medium-size business channel, with much of it driven by the Paysafe's agreement with Fiserv Inc. to peddle Fiserv's popular Clover point-of-sale technology to merchants.

"We're doing really well selling Clover," Lowthers said, estimating the technology has helped drive sales in the small-business channel by a "low teen" percentage year-over-year." Overall, Paysafe's merchant business will "grow robustly" this year, predicted chief financial officer John Crawford during the call, though he added, "Gross profit will be more robust in the second half than the first half." Crawford took over as CFO in September.

The coming months will also lead to a more mature, larger, and better-prepared sales team, Lowthers promised. "I feel good about the people we're bringing on board as they ramp up," he said. "2025 will be about continuing to ramp them up, continuing to bring maturity to that organization."

Digital wallets, which account for 48% of Paysafe's business, delivered 4% revenue growth last year, slowing down from 7% in 2023 but a turnaround from a 7% slide in 2022, according to numbers released for the call. The merchant-acquiring line of business grew 6% last year, a slight slowdown from 2023, while the company's e-commerce revenue surged 30%, slightly more than the growth in 2023 and an about-face from a 3% drop in 2022. E-commerce processing accounts for 10% of Paysafe's overall business.

Lowthers said 2024 represented the "completion of our turnaround" from the position he found the company in when he took over in 2022. Now, he said, Paysafe can "focus on sales-cycle productivity."

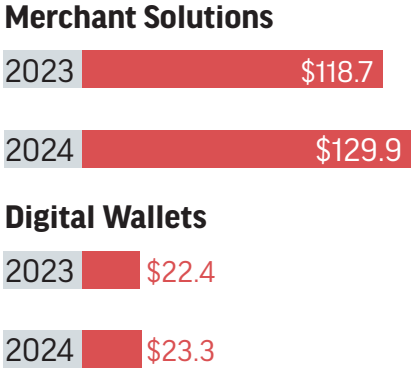
Payments volume came to $40 billion for the December quarter, up 12% year-over-year, and $151.7 billion for the year, an 8% rise. The fourth-quarter result came despite an $11-million "headwind" from "disposed businesses," the company said. Revenue for the quarter totaled $420.1 million, up slightly more than 1%; for the year, $1.7 billion, up 6%. Adjusted net income for Paysafe as a whole in 2024 dipped 8% to $132.5 million.

Overall, declared Lowthers, "I'm more optimistic today than I was three years ago when I joined Paysafe."

— John Stewart

PAYSAFE'S PAYMENTS DRIVERS

(Dollar volume in billions)



Source: Paysafe

RANDOMNESS IS BETTER THAN MATH

BY GIDEON SAMID
gideon@bitmint.com

WE WERE ALL fascinated, and perhaps intimidated, in school when we learned Euclid's geometry and the way he was able to prove statements and declare facts that exceeded human experience.

Euclid did not draw all possible triangles to measure and verify that any and all triangles will have exactly 180 degrees for the sum of their angles. He used mathematical logic to back up his claim. And indeed, for thousands of years ever since no one was able to draw a triangle on a flat surface such that the sum of its angles was 179 degrees, or 181 degrees. And nobody is concerned today that the emerging quantum computers will defeat this ancient Greek mastermind. That is why we regard math with such admiration and a sense of awe.

Comes now something called "mathematical money," most notably Bitcoin. It is built on a mathematical foundation. What could have been better?

Some call Bitcoin "digital gold." This is rather misleading. Gold is tested against all sorts of acids and other chemical reagents. Most of us are not chemists, but we trust and believe that gold cannot be chemically corrupted. Likewise, most of us are not mathematicians, but we trust that the mathematical foundation of Bitcoin is as solid as Euclid's geometry.

Surprisingly, perhaps, this is not the case. Unfortunately, though, very smart, highly respected individuals with solid cryptographic credentials are insisting that the mathematical foundation of common digital coins is unassailable. Imagine that, instead of offering a proof, Euclid had come forward and said: "I have been drawing hundreds of triangles and all of them had 180 degrees, so being smarter than anybody else I know, it is clear that no one can draw a triangle with other than 180 degrees."

This would not have cut it, and we would not have celebrated Euclid as the great mathematician he was. But this is exactly what contemporary mathematicians are saying about Bitcoin and its ilk: "We tried to crack it and failed, so how would lesser mathematicians put us at risk?"

What protects Bitcoin, Ethereum, Tether, and their like is not a mathematical barrier, but an innovation step. Bitcoin traders claim "In algorithm we trust," meaning, we bet on mathematics. This is mathfalsification. Bitcoin traders, in fact, bet against innovation. In this day and age, it is more than a tad ironic, but it is legitimate: people bet for and against many things. What is important is to make it clear. Cigarettes are sold freely, but with a cancer warning. Bitcoin should be traded freely, but with a clear warning that someone may be smart enough to cross this innovative step, and void all the wealth captured by its math.

It was refreshing to hear David Sacks, the new Czar for Crypto and AI, admitting in a Fox interview that if the Bitcoin innovative step were negotiated, Bitcoin would lose all its value, adding that, for now, there is no known success.

The people who wish to cast Bitcoin as a dollar alternative are desperately trying to hide this vulnerability. Many claim that the fantastic benefits of digital money should justify betting against innovation. They are wrong. All the benefits of digital money can be claimed by a different digital currency that relies on randomness rather than on unproven math.

Randomness can deliver what math can't. Randomness is the cyber equivalent of the material gold, indestructible, durable, shining. Its story will come in a future column.

The fascinating account of how randomness defeats math is presented in my new thriller, "The Cipher Who Came in From the Cold." DT

Simplified Security, Maximum Protection

PAYMENTS FOR RESTAURANTS

Magensa Cloud Services offer cutting-edge security for payments, acess, and authentication.

Services

- Magensa Payment Protection Gateway
- Magensa Decrypt and Forward
- Magensa Decrypt
- Magensa TokenExchange

More Ways to Pay

- Apple® Pay and Google® Pay
- PayPal® and Venmo®
- QR Codes and Links
- Hosted Payment Pages
- eCommerce
- Loyalty Tokens
- Subscriptions
- Invoicing
- Swipe, Tap, Dip, Manual, Over the Phone

Learn More About
Magensa
Cloud Services

DynaFlex II Go
with optional charging cradle

DynaFlex II Go

Mobile | Counter | Kiosk

For Secure Payments and Authentication.

MAGTEK®
SECURITY FROM THE INSIDE

Showcasing KwickPOS Solution with MagTek's DynaFlex II Go.

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

REFORM—DON'T ELIMINATE—THE CFPB

BY BEN JACKSON
bjackson@pa.org

AFTER THE ELECTION, many in the payments industry hoped the Consumer Financial Protection Bureau would be eliminated. While it does not seem like that will happen in the immediate future, the power of the Bureau has been curtailed. But where do things go from here?

With its nomination of a new director, the administration seems to have signaled it expects the agency to be around for at least a little while. Jonathan McKernan's nomination to be the director of the Consumer Financial Protection Bureau passed the Senate Banking Committee on March 6 in a 13-11 party-line vote. Treasury Secretary Scott Bessent was appointed acting director on Jan. 31, following the dismissal of Rohit Chopra. On Feb. 8, Office of Management and Budget director Russell Vought took over as acting director. Much like other cabinet nominees, McKernan likely will be confirmed by the Senate in a party-line vote.

It is important to remember that the CFPB was created by the Dodd Frank Act. Since it is a product of legislation, eliminating the agency will require new legislation. But as long as Elizabeth Warren is in the Senate, we can expect any bill that would eliminate the agency would meet with a filibuster.

But the administration does not need a law to eliminate the agency as a regulator. Instead, the administration's current strategy seems to be to reduce the Bureau's power by eliminating its staff and resources.

When Bessent took over, he told staff not to do any work unless it was approved by the director or required by law. Since then, mass layoffs of Bureau staff have resulted in a lawsuit over the firing of staff. In addition, the CFPB appears to be pulling back in other ways. It has dropped at least six lawsuits that it had filed before the new administration took office, including actions against Capital One, Rocket, Homes, Pennsylvania Higher Education Assistance Agency, Vanderbilt Mortgage and Finance, and Heights Finance Holding Company.

In March, the CFPB said it was dropping its lawsuit against Early Warning Services, which operates the peer-to-peer payments service Zelle, along with three of its owner banks—Bank of America, JPMorgan Chase, and Wells Fargo, "with prejudice," according to CNBC. In December, the CFPB sued Early Warning Services, along with the three banks, alleging that the companies did not investigate fraud and reimburse consumers for fraud and error.

While an empty CFPB might seem like a good option for the industry, there are risks to a skeletonized Bureau. An effectively closed CFPB will not be making any changes to the rules that do exist. This means rules cannot be updated for new technology, and the industry cannot get modifications to existing rules that would benefit both them and their customers.

Regardless of the status of the agency itself, the rules it has written are still on the books. This means every company is at risk of the broken-taillight theory of enforcement. The short version of this meme is that getting pulled over for a broken taillight can lead to all sorts of other legal problems. If a regulator does an exam and notices one problem, examiners can use rules that were originally under the purview of the CFPB to add to the compliance headaches.

Lawsuits filed by customers might also use the existing regulations to make a case against companies. And the states might try to make up for a perceived gap in federal enforcement.

The optimal outcome is a CFPB that acts with restraint and works with the industry so that both sides have the common goal of protecting consumers while promoting innovation. DT

3 EASY WAYS TO MAKE MORE MONEY

Simple changes to earn a better residual with SignaPay

Let's face it, as salespeople, our goal is to sell more to make more. That's why SignaPay makes it easy to earn a better residual in 3 easy ways. Beyond that, we as your full-service ISO, we provide all the tools you need to sell your merchants a better product.

SELL PAYLO

The leading compliant Dual Pricing program not only earns you up to 3 times more in residuals, but gives your merchants the confidence and trust in a program backed by the major card brands.

GET PAID YOUR WAY

When you become a SignaPay Partner, you unlock access to build your residual payout how you want it to be. Earn more through bonuses or a higher revenue split. The choice is yours!

SELL MORE VERTICALS

From Online Retail, to CBD Shops and more, we accepts merchants of all kinds, big and small, old and new.

Plus many more ways to earn more...

$1,000 ACTIVATION BONUS • BUSINESS LOANS • RESIDUAL PURCHASES • MARKETING TOOLS & SUPPORT
FREE TERMINALS • 90% RESIDUAL SPLITS • ONLINE E-APP • ONE-CLICK APPROVALS • 24/7 SUPPORT

SIGNAPAY | PAYLO

Sign up today.

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

THE ABCs OF ONBOARDING KPIs

Getting the merchant onboarding process right means merchants encounter no obstacles and acquirers get the data they need—fast.

BY **KEVIN WOODWARD**

AUTOMATION HAS NOT only changed the quality of merchant data, it has change how quickly merchants provide it during the onboarding process. Now, as artificial intelligence tools stream into the acquiring industry, the demand for an expedient and accurate onboarding procedure is intensifying, just as the number of payment facilitators and payment service providers courting merchants, too.

With new tools becoming available and the need for speed intensifying, the criteria for assessing performance in the onboarding experience becomes even more critical.

"Effective merchant onboarding is complex because it must balance the needs of the payments companies with the desires of the merchants," says Andry Vrabel, general manager of payment ecosystem solutions at LegitScript LLC, a Portland, Ore.-based merchant risk and monitoring services firm.

"Payments companies want thorough checks to ensure a prospective merchant isn't going to engage in brand-damaging or illegal activity," continues Vrabel, "while merchants want a quick and easy process so that they can start selling."

As Matt Bennett, vice president of partnerships and alliances at FICO, puts it, "The primary objective of a merchant-onboarding process is to simplify the workflow and deliver a seamless customer experience." FICO is a Bozeman, Mont.-based data-analytics provider.

THROUGH THE FUNNEL

Measuring how well that task can be done relies on common key performance indicators, or KPIs. Bennett lists nine KPIs, a few of which include time to activation, approval and abandonment rates, costs, and satisfaction scores. For his part, Vrabel lists speed, the completion rate, user experience, and friction and bottleneck analysis.

"Funnel pull-through rates are one quantitative indicator that helps us understand ease as we look at how many merchants start the process versus how many complete all the way through to taking payments," says Jessica Young, managing director and head of product at Chase Payment Solutions. "Another key metric is direct client feedback on their onboarding experience, for example as measured in client-facing surveys and research."

The funnel pull-through rate refers to the percentage of a merchant cohort that ultimately completes the onboarding process, Young says. "For example, if 100 merchants enter the onboarding flow but only 70 make it to the final screen, we would consider that a 70% pull-through rate," she says.

"We spend time looking at each step of the journey to see drop-off rates on every page of the flow. If a particular screen has a higher drop-off rate, that suggests opportunity to improve that experience to improve overall funnel pull-through," Young adds.

Chase, like other acquirers, wants to know how long it takes a merchant to complete the process. "Specifically, we want to ensure merchants who onboard are ultimately transacting and that we have put in the right upfront checks and responsible friction in the process to identify and prevent bad actors," Young says.

Generally, each of these metrics is as important as another, observers say, though time to activation may be most critical. "It provides fast and seamless onboarding, allowing merchants to start generating revenue sooner, which impacts both their success and the acquirer's growth," Bennett says.

As Vrabel explains, "No one factor, on its own, is paramount in an effective merchant onboarding process," he says. "A fast solution is useless if it isn't accurate, and an accurate solution has limited use if it is rigid and unable to scale. That's why it's essential to balance the need for accurate analysis with the industry pressure to vet and approve merchant applications quickly."

Using accuracy as an example, Vrabel says automated merchant category-code detection, know-your-business checks, and other data can help. The MCC is typically a four-digit number. "Our research suggests that 40% of merchants are miscoded. The most commonly misused MCCs are 5734 and miscellaneous MCCs ending in 99," Vrabel says.

AI'S IMPACT

Though automated onboarding services have been available for a while, the introduction of artificial intelligence may be an accelerant and could put more emphasis on onboarding metrics.

"Automation is increasingly vital in merchant onboarding, helping payment acquirers onboard merchants faster while implementing stronger know your customer (KYC) and due-diligence practices," says Mary Clair Williams, vice president of product management at G2 Risk Solutions Inc., a Burlingame, Calif.-based risk-management provider. "It is why many acquirers have been able to grow merchant portfolios and reduce risk exposures simultaneously."

It is not hyperbole to say that AI is having a transformative effect, Williams says, "and its impact will only continue to grow as acquirers work to balance speed with risk mitigation."

The additional utility of AI is manifold. "AI can synthesize billions of data points to produce a nearly instantaneous risk score, in that interest. This comprehensiveness goes far beyond the capabilities of traditional underwriting processes," Williams says. "Moreover, AI can do


Vrabel

Vrabel: "A fast solution is useless if it isn't accurate, and an accurate solution has limited use if it is rigid and unable to scale."


Williams

Williams: "AI helps acquirers conduct continuous merchant monitoring, critical for maintaining a secure portfolio."

this without creating unnecessary friction for legitimate businesses, which is increasingly essential in the highly competitive payment-services landscape."

LegitScript is one vendor with AI embedded in its merchant-onboarding product suite. Its Xray AI Risk Intelligence platform combines proprietary Website crawling and AI with its universe of risk data of more than 60 million merchants and billions of data points, Vrabel says.

"Our research team views AI as the future of merchant-risk management," he says. "Manual risk detection, though valuable for certain use cases, is slow, expensive, and unscalable, while traditional automation is inaccurate, inflexible, and limited. AI-driven solutions, however, can do things like instantaneously scan merchant Websites, automatically detect merchant category codes, and learn and adapt as rules change."

The role of AI, or machine learning, is critical at acquirers like Chase Payment Solutions. "Machine learning is a key capability when it comes to risk and fraud models. As we gather data on merchant profiles and behavior, the models get smarter and help to identify merchant onboarding applications that require further review," Young says.

Bennett agrees, adding, "Yes, artificial intelligence can play a transformative role in merchant onboarding by improving speed, accuracy, and user experience while reducing manual efforts."

Among the roles AI can fill are identity and compliance verification, he says. It can help with automated document recognition, facial recognition and liveness detection, and instant KYC and anti-money laundering compliance checks. It also can help with pricing, intelligent risk assessment, and fraud detection during the onboarding process.

Other uses include powering chatbots and text-based assistance, and automated agreement generation and e-signature demands, Bennett says.

VETTING VENDORS

Another key metric is assessing the performance of onboarding services providers. At LegitScript, Vrabel, as a vendor, says third-party providers should "have a demonstrated history of accuracy, accountability, and transparency."

Bennett suggests evaluating providers on the ease of integration, scalability, adherence to security and compliance standards, and the user experience. Also, the configurability of the platform, its cost effectiveness, customer support and service-level


Young

Young: "As we gather data on merchant profiles and behavior, the models get smarter and help to identify merchant onboarding applications that require further review."


Bennett

> Bennett: Watching time to activation "provides fast and seamless onboarding, allowing merchants to start generating revenue sooner, which impacts both their success and the acquirer's growth."

agreements, and reputation and track record, complete his criteria.

AI's role is not just for the initial onboarding steps, but can factor into ongoing merchant monitoring.

"Beyond onboarding, AI helps acquirers conduct continuous merchant monitoring, critical for maintaining a secure portfolio," Williams says. "Onboarding is one part of the merchant lifecycle, and payment providers must ensure compliance throughout its entirety. AI tools are never 'off the clock.' They constantly ingest information and can detect complicated behavioral patterns and suspicious activity that a merchant may attempt to conceal." DT

THE HIDDEN COSTS OF POOR SPEND MANAGEMENT

Making back offices more efficient may well deliver more savings than you think.

BY SHAZ KHAN

Shaz Khan is co-founder and chief executive at Vroozi.

IMAGINE FINDING OUT your company is spending $40 to process a single invoice. Now multiply that by thousands of invoices per month. If that sounds insanely high to you, you're right. But it's happening right now in enterprises across America.

I recently spoke with a procurement leader who had just discovered this exact situation. The organization were spending more to process some invoices than the actual items being purchased. In some cases, these were routine office supplies costing less than $20, yet the administrative overhead was double that amount.

This is not an isolated case. In boardrooms nationwide, executives are discovering the true cost of what I call the "corporate credit card culture." Without controls, preferred vendors, or spending visibility, organizations are leaving millions in potential savings on the table. The problem has only intensified with the rise of remote work and decentralized purchasing, creating a perfect storm of inefficiency and waste.

As someone who has worked with countless enterprises to modernize their spend management, I've seen firsthand how the "Wild West" approach to corporate spending is costing companies millions.

Picture this common scenario: employees are handed corporate credit cards with $2,000 limits and told to "buy what they need." No controls, no preferred vendor relationships, no visibility into spending patterns. It's a recipe for waste and compliance nightmares. Even worse, this approach often leads to duplicate purchases, missed volume discounts, and a fragmented supplier base that diminishes purchasing power.

THE COST OF INEFFICIENCY

Let's talk numbers. When fully loaded with all systems, tools, and personnel costs, processing a single purchase order can cost anywhere from $80 to $250. Invoice processing isn't much better, often running $15 or more per document. These are not just statistics – they represent real money being spent on manual processes, disconnected systems, and inefficient workflows.

Consider the hidden costs: time spent reconciling statements, tracking down approvals, managing vendor relationships, and dealing with exceptions. Each step adds to the total cost of processing.

But here's what's even more worrisome: Most companies don't even measure these costs. They know it takes forever to get a purchase order out or pay a supplier, but they've never calculated the true impact on the bottom line. Some accounts-payable departments are staffed with dozens of people performing manual tasks that could be automated, driving costs even higher.

The ripple effects extend throughout the organization, from delayed projects waiting for purchases to strained vendor relationships due to payment delays.

What's particularly frustrating is that these ineff iciencies often persist simply because "that's how it's always been done." Organizations continue to throw people at the problem instead of addressing the root causes of their spend-management challenges. To address these mounting ineff iciencies, leading organizations are turning to a proven framework that transforms how they manage their business spend.

THE THREE Cs

This framework centers on three fundamental pillars of modern procurement: control, consolidation, and compliance. These principles aren't just theoretical. They're built into most chief procurement off icers' mission statements because they consistently deliver measurable results. When properly implemented, they create a virtuous cycle of eff iciency and savings.

Control: Modern spend management means establishing clear processes and approval workfl ows. Instead of the "Wild West" of corporate credit cards, organizations need systems that guide purchasing decisions while maintaining speed and agility. This means automated approvals, clear spending limits, and real-time visibility into all transactions.

The key is finding the right balance. Too much control creates bottlenecks, while too little leads to waste. Advanced systems can adapt approval workflows based on risk levels, employee roles, and spending patterns.

Consolidation: By consolidating suppliers and creating a single source of truth for all spending data, companies can leverage their buying power and negotiate better contracts. More importantly, they can ensure employees are using preferred suppliers with pre-negotiated rates instead of making one-off purchases at higher prices.

This consolidation extends beyond just vendor management. It means bringing together all spending data, contract information, and supplier relationships in one unified platform. The insights gained from this consolidated view often reveal surprising patterns and opportunities for optimization.

Compliance: Every purchase should align with company policies and procedures. This isn't about creating bureaucracy. It's about protecting the organization while maintaining efficiency.

Modern digital systems powered by artificial intelligence can enforce compliance automatically


Khan

Khan: "Imagine explaining to your board why you're spending nearly half a million dollars annually just pushing paper around."

without slowing down the procurement process. They can flag potential policy violations, identify suspicious patterns, and ensure regulatory requirements are met without human intervention. This approach prevents issues before they occur, rather than discovering problems during audits.

COST CENTER TO VALUE DRIVER

The good news? With today's AI-powered spend-management platforms, companies can reduce their processing costs dramatically with intelligent document scan and capture and automated approvals.

Best-in-class organizations process purchase orders for under $15 and invoices for under $3. That's not just incremental improvement. It's a fundamental shift that goes straight to the bottom line. These platforms don't just automate existing processes. They reimagine them from the ground up.

Consider a company processing 10,000 invoices monthly. At $40 per invoice (a real figure reported by one organization I recently spoke with), they're spending $4.8 million annually just on processing. Reducing that cost to $3 per invoice would save $4.44 million. That's money that could be reinvested in growth initiatives or dropped straight to the bottom line.

And this is just the direct cost savings. The indirect benefits, such as better cash management and stronger supplier relationships, often exceed the immediate financial impact.

While these cost savings are compelling, the benefits extend far beyond efficiency. Modern spend management enables:

- Faster processing times (from days to minutes);
- Better supplier relationships through prompt payment;
- Enhanced visibility into spending patterns;
- Stronger compliance with regulatory requirements;
- More strategic allocation of AP and procurement resources;
- Improved cash flow management and working capital optimization;
- Better negotiating positions with suppliers through consolidated purchasing data;
- Reduced risk of fraud and policy violations

For chief procurement officers and financial officers, this isn't just about running a tighter ship. It's about delivering measurable value to the organization. When teams can show millions in savings through more efficient processes and better supplier management, everyone wins. The procurement function transforms from a back-office necessity to a strategic driver of business value.

TIME FOR CHANGE

The technology exists to change spend management from a cost scenter into a strategic advantage. Organizations can move from manual, paper-based processes to intelligent, digital workflows that enforce compliance while accelerating business.

The question isn't whether to make this transition, but rather how quickly you can get started. The competitive landscape demands it. Companies that cling to outdated processes will find themselves at an increasing disadvantage.

Think back to that $40 invoice-processing cost. Now imagine explaining to your board why you're spending nearly half a million dollars annually just pushing paper around, when your competitors are doing the same work for a tenth of the cost.

Modern spend management isn't just about efficiency. It's about survival in a world where every dollar counts. The technology exists. The roadmap is clear. The only question is: will you be the hero who saved your company millions, or the one who has to explain why you didn't?

The path forward goes beyond just implementing new technology. It's about reshaping your organization's relationship with money itself. It's about building a workplace where every dollar serves its highest purpose, where control and agility work in harmony, where compliance enhances rather than hinders efficiency.

The companies that embrace this evolution won't just survive – they'll become the new standard against which others measure themselves. DT

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

AI TAKES TO THE FRAUD PREVENTION FIGHT

Criminals' increasing adoption of artificial intelligence to power fraud schemes is leaving merchants and payment providers little choice but to adopt the technology to fight back.

BY PETER LUCAS

ARTIFICIAL INTELLIGENCE HAS MADE THE FRAUDSTER'S JOB EASIER. NOT ONLY HAS AI IMPROVED THE QUALITY AND SOPHISTICATION OF HIS ATTACKS, IT'S NOW EASIER THAN EVER FOR CRIMINALS TO ACCESS THE TECHNOLOGY THROUGH MARKETPLACES ON THE DARK WEB.

Hence, any wannabe criminal, even one with limited resources, can find advanced tools to beat identity-verification and fraud-detection systems—at prices lower than they were just a few years ago, fraud-prevention experts say.

Criminals can use AI to deploy bots for rapid card testing and credential-stuffing attacks, launch sophisticated phishing campaigns that capture login credentials or personal and financial data, and create synthetic identities so realistic they can fool identity-verification systems.

Indeed, AI has handed fraudsters such an edge that 84% of fraud-prevention professionals at financial institutions say the technology can beat their current fraud defenses, according to a recent study by Datos Insights. It has also helped create a criminal enterprise that represents a nearly a $10-trillion economy, says Mastercard Inc.

As a result, the threat of fraud from the use of AI is extremely high. On a scale of 1 to 10, with 10 being the most serious, "I would rate it an 8," says Sunny Thakkar, senior director of product management, fraud, disputes, and authentication at Worldpay Inc.

Indeed, thanks to criminals' adoption of artificial intelligence, losses from cyberfraud rose 14% in 2024, according to a report from Trustpair, a provider of fraud-prevention technology.

"Cybercriminals' increasing sophistication and use of AI is a growing concern, as highly sophisticated AI is available to the general market and continues to get more and more advanced," Thakkar says. "We are monitoring this threat with extreme caution."

'A DOUBLE-EDGED SWORD'

While AI has given fraudsters an edge, that doesn't mean processors, networks, and card issuers are defenseless against fraud. Rather than develop a new technology to combat AI-based fraud, the payments industry is recognizing that AI can be used to turn the tables on criminals and strengthen its own fraud defenses.

What makes AI an effective fraud-fighting tool is that it uses predictive analytics to detect emerging patterns and adapt to those patterns—in real time. AI can also aggregate and interpret multiple data attributes, such as device data, email address, IP address and physical address, to detect any red flags in a given transaction.

Using AI, merchants can increase approval rates by declining fewer legitimate transactions. These are transactions that would have been declined using less sophisticated fraud-detection technologies. And all while catching more fraudulent transactions.

"Advancements in AI, coupled with robust data, are revolutionizing fraud prevention, making [AI] a double-edged sword," Thakkar says. "AI is both an asset and a threat, and is one of the areas I continue to watch closely."

But before processors, networks, and payments providers can use AI to beat fraud, they need to understand how the technology is being used to commit fraud in the first place, industry experts say.

AI's ability to rapidly analyze vast fields of data makes it an effective tool for creating synthetic identities. These IDs, which can be used to open a credit card account or take out a loan, for example, are forged using valid consumer data stolen in a data breach—such as Social Security Numbers—paired with personally identifiable information that is often false.

Synthetic identities can be so realistic that many card issuers don't realize they are falling prey to them. Indeed, it is not uncommon for issuers to incorrectly assume a delinquent account opened with a synthetic identity went bad for reasons other than fraud.

"Financial institutions don't do a great job of getting at the root source of the fraud to combat it," says David Mattei, a strategic advisor at Datos Insights. "FIs will write off an account that goes bad as a loss without necessarily drilling down to see whether the cardholder's identity is real."

'FRAUD-AS-A-SERVICE'

Another growing use of AI for fraud is fraud-as-a-service, a cybercrime business model where a criminal provides the necessary tools and services to other criminals seeking to perpetrate fraud. FaaS opens the door for any individual to commit fraud, regardless of his expertise.

The problem for banks and payments companies that attacks mounted by individuals or small groups tend to be smaller in scope and therefore harder to detect than attacks orchestrated by large fraud rings.

"FaaS doesn't require specific fraud skills [of the user], which gives individuals and small groups the ability to perpetrate fraud more effectively," says Ofer Friedman, chief business development officer for Au10tix, an Israel-based identity-verification firm. "FaaS is like autopilot. The user tells the provider what they want" and it gets served up.

Making matters worse is that many FaaS providers actively advertise their services on the dark Web.

"Fraud-as-a-service is leveraging AI to scale and automate fraud, making sophisticated AI-driven fraud patterns accessible to a wider pool of criminals," says Laura Quevedo, executive vice president, fraud and decisioning solutions, at Mastercard.

"AI tools can create synthetic identities and bypass traditional know-your-customer [practices] and infiltrate payment systems," she adds. "These techniques facilitate automated payment fraud and advance money laundering."

'A HUGE PROBLEM'

The use of AI to facilitate the opening of money-laundering accounts is a growing problem for financial institutions. It is not uncommon for criminals to open a so-called mule account and funnel through that account money scammed from consumers through phishing attacks or social engineering.

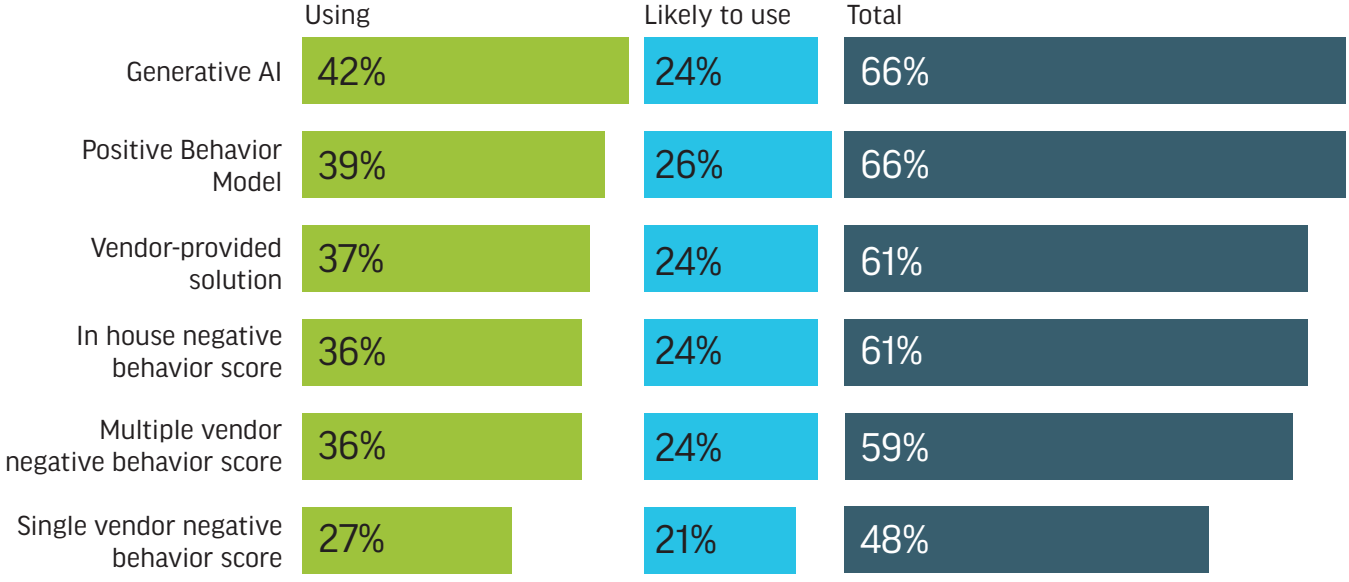
"While banks typically didn't worry about mule accounts on the payments side of the house because they didn't lose money on a transaction, concern is growing on the money-receiving side of the bank about them," says Mattei.

AI can help banks identify mule accounts by analyzing in real time transaction and accountholder behavior patterns, as well as other anomalies, Mattei adds.

But AI-based tools aren't only being used to perpetrate consumer fraud. Criminals are using them in the business-to-business payments space, too, where transaction sizes are substantially larger. In 2024, AI was involved in

GENERATIVE AI RANKS HIGH FOR FRAUD PREVENTION

(Percentage of merchants using or likely to use each tool)



Note: Results of survey of more than 1,100 merchants globally
Source: Visa's 2024 Global E-Commerce Payments & Fraud Report

25% of the cases in which a business lost $10 million or more due to fraud, according to Trustpair, a provider of fraud-prevention technology.

One attack vector in the B2B space is for criminals to take over a vendor's email account using AI-based tools, then notify buyers in the vendor's email address book that the account number to which payments are made has been changed. The notice of course adds that buyers should send future payments to the new account, which the criminal controls.

With AI, criminals can not only gain access to email accounts, they can see all correspondence with those accounts to identify which ones to target, such as those that have an invoice due soon.

"Generative AI can make illegitimate emails difficult to identify, especially for smaller companies that have limited technology resources," says Baptiste Collot, chief executive at Trustpair. "A lot of businesses use manual processes for validation, and that is becoming a huge problem with the use of AI by criminals."

MASTERCARD'S APPROACH...

Not surprisingly, larger players such as Mastercard and Visa Inc. are actively getting out in front of the fraud threat posed by AI.

Mastercard's real-time decisioning solution, known as Decision Intelligence, uses Generative AI to scan 1 trillion data points to predict whether a transaction is likely to be genuine or not. The operation takes less than 50 milliseconds.

The app, which scores and approves 159 billion transactions a year, can boost fraud-detection rates by an average of 20%, and as much as 300% in some instances, Mastercard says.

Other AI-based-fraud fighting solutions used by Mastercard include the network's Safety Net technology to protect against fraud and cyber-attacks. The technology has prevented nearly $50 billion in potential customer fraud losses from attempted global fraud and cybercrime attacks across Mastercard's network over the past three years.

Mastercard also employs identity solutions to spot synthetic identities being used to open an account and to share fraud and disputes data to speed up the resolution process for merchants, issuers, and consumers.

"We have long recognized the importance of delivering technology to stay ahead of criminal activities to protect banks, businesses, and consumers worldwide," Quevedo says. "This technology helps us know where the fraudsters are operating so we can act swiftly to help protect banks and consumers."

Mastercard further bolstered its AI-based fraud-prevention capabilities through the acquisition last year of Recorded Future Inc. The company uses AI to analyze broad data sets to provide real-time insights to help mitigate risk.

"Mastercard's acquisition of Recorded Future will further enhance our threat intelligence, enabling us to create smarter models to better protect organizations, consumers, and the ecosystem as a whole," says Quevedo.

...AND THAT OF OTHERS

Like Mastercard, Visa has deployed an array of AI-based fraud-detection tools. These include cardholder-authentication apps, support for token-provisioning requests, fraud detection for account-to-account payments for financial institutions, and scoring a transaction to determine whether it is part of an enumeration attack.

Collot: "Too many think they will find a long-term answer [to fighting fraud], but no solution is good forever."

An enumeration attack occurs when criminals try to gather information about a system by testing various inputs of consumer data to identify valid usernames, email addresses, or other data points within a database. Visa did not make executives available for comment on these tools.

Payments providers like Worldpay are also investing heavily in AI. Worldpay's FraudSight is a multi-layered solution that combines data insights, technology, as well as a team of fraud experts and data scientists to predict the types of transactions at high risk for fraud.

Acquisitions, too, are helping Worldpay build out its fraud-fighting technology stack. Earlier this year, the payments provider entered into an agreement to acquire Ravelin Technology Ltd., a provider of fraud-prevention solutions for e-commerce merchants. Terms were not disclosed.

Ravelin specializes in identifying payments fraud—account takeover, return and refund abuse, promotion and voucher abuse, and marketplace fraud—and in 3D Secure authentication. The acquisition will enable Worldpay merchants to increase authorizations, the company says.

"In e-commerce, the cost of customer acquisition is higher than ever, yet merchants face lower overall approval rates as transactions are susceptible to more fraud and higher issuer declines," says Worldpay's Thakkar. "Given the need for higher approval rates to maximize retention of revenue, merchants are applying continued pressure for payment providers to maximize authorization rates."

E-commerce merchants' need to effectively combat fraud has made AI a "survival" technology, for payment providers, according to Thakkar.

"Nearly all the top payment providers are applying AI in their business, with AI-based fraud detection being a critical component in merchants' achieving higher approval rates," Thakkar adds.

VETTING VENDORS

When choosing an AI-based fraud-detection provider, it is important to dig beneath the sales pitch and get a demonstration of the technology, as well as talk to other users about how the effectiveness of the vendor's solution and whether it is meeting their needs and objectives, says Datos Insights' Mattei.

Au10tix's Friedman also recommends working with established AI vendors. "Go with known players in the space that can run a proof of concept," he says.

Vetting vendors is just one step in the process of using AI to fight fraud. The exchange of data, internally and industrywide, is viewed as critical to making sure AI-based fraud-prevention tools keep pace with cybercriminals' changing use of the technology. This means keeping in mind that AI is a data-driven solution.

"The more data available, the higher the accuracy in the risk decision. That's one reason collaboration within the payments industry and building a strong ecosystem are important best practices," says Thakkar. "We're starting to see a lot more partnerships across the ecosystem to create more robust frameworks for data sharing to improve outcomes for every payment."

Working with issuers such as Capital One, Worldpay has developed an application programming interface that securely packages information so that when the authorization reaches the issuer, the issuer can see the data linked to a transaction. Such information helps improve the issuer's confidence in approving the transaction, Thakkar adds.

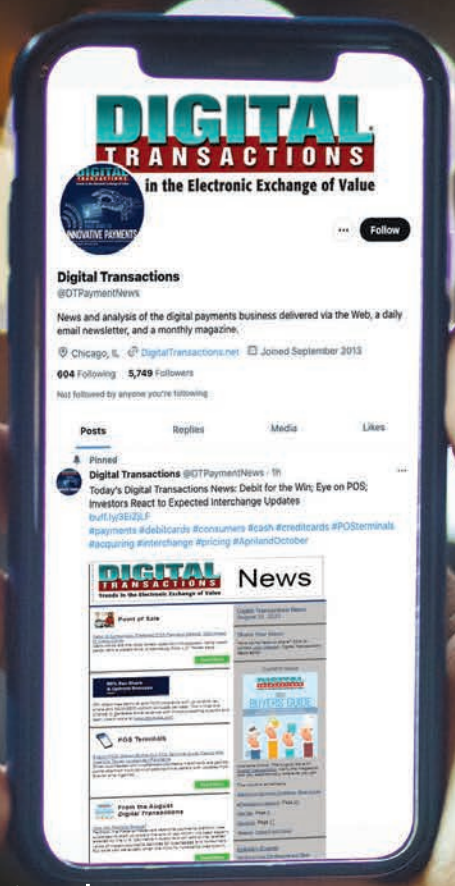
Lastly, payment providers need to set realistic goals with an eye for the long-term when developing an AI-based fraud-prevention strategy. "Start small, but think long-term and be prepared to grow with change," says Trustpair's Collot. "Once you get through the initial steps, you can start to think bigger. Too many think they will find a long-term answer [to fighting fraud], but no solution is good forever."

To stay ahead of evolving threats, he adds, "You need to be constantly looking ahead." DT

Mattei: "Financial institutions don't do a great job of getting at the root source of the fraud to combat it."

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

Today and every day follow
DIGITAL TRANSACTIONS
@DTPAYMENTNEWS on X



Do not be left behind.

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

CAN STABLECOINS BRIDGE THE PAYMENTS LIQUIDITY GAP?

Digital currency could solve some knotty problems plaguing cross-border payments.

BY **NKIRU UWAJE**

Nkiru Uwaje is chief operating officer and cofounder at MANSA.

A CHASM PERSISTS within payments liquidity, posing a significant challenge for payments companies and fintechs providing cross-border transactions.

Traditional models, which rely on prefunded accounts and correspondent banking networks, have demonstrated that they are often inefficient and costly. In 2023, the global average cost of sending payments to low and middle-income countries was 6.2% per transaction, significantly higher than digital-payment alternatives.

Despite advances in fintech technology and the development of inventive techniques to sidestep traditional international payments infrastructure, liquidity constraints remain a bottleneck, limiting the speed and efficiency of global payments.

Enter stablecoins—virtual assets that maintain a stable value relative to a specific asset, typically a major global currency like the U.S. dollar or the euro—which now offer a novel solution to this ongoing challenge. As stablecoins gain traction in mainstream financial applications, they are emerging as a tool to enhance liquidity and enable real-time settlements for cross-border payments providers.

PREFUNDED LIMITATIONS

Most cross-border payments systems operate on a prefunded basis. Payment service providers (PSPs) must maintain liquidity in all supported jurisdictions, locking up capital to facilitate transactions.

This approach presents several challenges for payments companies. First, it is immensely capital-inefficient, and businesses often have to tie up significant funds in

multiple accounts across regions and currencies. These accounts are often subject to significant market fluctuations, which reduces the ability of businesses to allocate resources dynamically.

Cross-border payments revenues reached $240 billion in 2022, a 17% increase from the previous year. The rising transaction volumes inevitably cause an increase in operational complexity, with payments companies struggling to increase their liquidity in all jurisdictions as demand for payments rises and falls in an unpredictable manner. In addition, each jurisdiction enforces its own version of cumbersome compliance and reconciliation requirements.

Alongside these concerns are a number of high costs for stakeholders. Banks and PSPs incur high fees from intermediary banks, impacting both businesses and consumers.

Given these constraints, the industry is actively seeking alternatives that allow real-time access to liquidity without requiring large capital reserves.

'REAL-TIME' SETTLEMENTS

In traditional cross-border transactions, "real time" often refers to payment initiation rather than actual settlement. Legacy banking systems typically take two to three days for final clearing, with intermediaries adding further delays. True real-time settlement means instantaneous finality, where funds become available immediately upon transaction execution.

Stablecoins, particularly those pegged to fiat currencies, provide a mechanism for immediate transfer and settlement without reliance on multiple intermediaries. By leveraging blockchain technology, stablecoins offer an alternative to pre-funded accounts, providing instant liquidity when and where it is needed.

Liquidity is the backbone of financial transactions. Without immediate access to funds, businesses face various challenges incurred from delayed payments. These challenges include suppliers experiencing cash-flow issues due to delayed settlements, increased credit risk exposing businesses to counterparty risk, and smaller fintechs struggling to expand to new jurisdictions and compete with larger, more established institutions, due to capital constraints.

The International Finance Corporation estimates 65 million firms suffer from cash-flow issues due to late payments, restricting their ability to invest and grow.

Stablecoins provide a stark contrast, offering a decentralized and programmable approach to liquidity. In December, Starlink turned to stablecoins to address challenges in receiving payments from emerging markets. It used Bridge, acquired by Stripe, to accept transactions from all corners of the globe. Many businesses in emerging markets still face slow international settlements and high foreign-exchange fees due to reliance on traditional banking rails.

Through the use of stablecoins with blockchain networks, transactions that once took days through pre-funded accounts now settle within minutes, significantly improving liquidity and ensuring smaller businesses can compete with larger financial institutions. Liquidity challenges are always being addressed, but what we are seeing with stablecoins is the real-world introduction of a technology that rapidly enables greater financial inclusion for smaller players in the payments ecosystem.

PRACTICAL IMPLEMENTATION

It's one thing to laud the appropriateness of stablecoins as an alternative. A whole other challenge is working with stakeholders to integrate them into cross-border payments infrastructure effectively.

The first major consideration is compliance—how to navigate a complex regulatory environment to ensure adherence to anti-money-laundering and know-your-customer requirements. Related to, but not synonymous with, this process is ensuring that stability and security mechanisms are in place to mitigate volatility risks, particularly for algorithmic stablecoins.

Interoperability is another major challenge. Payment networks must support stablecoins seamlessly across different jurisdictions and financial infrastructures. Likewise, widespread adoption will require collaboration between fintechs, banks, and regulators to build trust in stablecoin transactions.

The future of stablecoins in cross-border payments will be shaped by several trends already playing out across the developed and developing world. One of the most significant developments is the rise of central bank digital currencies.

These could either compete with or complement stablecoins, with the latter potentially serving as an intermediary between traditional finance and state-backed digital assets. This is very much the order of the day in the world's most advanced economies. The digital Yuan is already a reality, and talk of a U.S. federal reserve of Bitcoin is now part of the economic zeitgeist.

A PROMISING SOLUTION

At the same time, programmable money is a significant catalyst for innovation in the payments industry. Smart contracts encoded within stablecoins and other cryptocurrencies can automate compliance, fraud detection, and risk management, thus removing friction from international transactions.

Parallel to this, decentralized-finance protocols continue to evolve, offering alternative liquidity solutions that bypass the constraints of the banking-infrastructure status quo.

Meanwhile, the financial sector is witnessing the emergence of institutional stablecoins, as major banks and corporations explore issuing their own digital currencies to streamline settlements and enhance transaction security. Together, these trends signal a shift toward a more integrated and versatile future for cross-border payments.

The payments-liquidity gap remains a critical hurdle in global finance, but stablecoins offer a promising solution. By enabling real-time settlements and seamless liquidity for pre-funded accounts, stablecoins can restructure the foundations of cross-border payments. As regulatory frameworks mature and industry adoption increases, stablecoins may become a cornerstone of a more efficient and inclusive financial system. DT


Uwaje

Uwaje: "The industry is actively seeking alternatives that allow real-time access to liquidity without requiring large capital reserves."

HOW DIGITAL TWINS UNLOCK INNOVATION

New services like real-time payments and open banking demand a real-time ledger alongside the core—a digital twin. Here's why.

BY CARLOS NETTO

Carlos Netto is chief executive of Matera

THE FINANCIAL-SERVICES industry is at an inflection point, driven by the rapid rise of real-time payments and consumer expectations for 24/7 banking. Legacy core-banking systems, while reliable, were not designed to handle the demands of instant payments, open banking, and artificial intelligence (AI).

As banks grapple with the challenges of modernization, one solution is emerging as both innovative and practical: the digital-twin approach.

A digital twin in financial services is a real-time transaction ledger that operates alongside a bank's core system. Unlike a traditional core replacement, which is costly and disruptive, the digital twin selectively replicates account data and handles transaction processing. It authorizes transactions, updates balances, and responds to inquiries in real time, whether the core is online or offline.

This approach decouples transaction authorization from the core, enabling banks to meet modern demands without overhauling their infrastructure. While the core continues to manage compliance, reporting, and complex calculations, the digital twin focuses on authorizing transactions, so customers enjoy around-the-clock access to banking services.

The need is urgent. Banks are losing ground to digital-first, nonbank competitors that excel in speed and convenience. Consumers expect banking services to match the immediacy of modern conveniences like food delivery and streaming.

However, legacy cores are often bottlenecks, holding up innovation.

The digital-twin approach is a low-risk, cost-effective way to modernize banking systems. By integrating a real-time transaction ledger, banks can address today's challenges while positioning themselves for the future.

USE CASES

Here are four key use cases that highlight the potential of digital-twin technology:

1. Instant Payments Without Replacing Your Core

Consumers increasingly expect instant payments to be available 24/7. Yet, legacy cores can struggle to meet these expectations due to their batch-oriented processing and limited uptime.

A digital twin addresses these challenges by:

- Authorizing transactions in real-time: Customers experience seamless payments regardless of whether the core is online;
- Updating balances 24/7: Balances are always accurate and available for inquiry, even during system maintenance or outages;

- Reducing costs: By handling transaction inquiries and balance updates, the digital twin minimizes expensive calls to the core system.

This approach enables financial institutions to launch real-time payment services like RTP or FedNow without overhauling their core infrastructure, providing a faster path to market.

2. Resiliency During Core Downtime

Banks must remain operational even when their core systems are offline for maintenance or because of unexpected outages. A digital twin ensures continuity by taking over transaction processing and balance updates during these times.

For example, during system upgrades, customers can continue making payments, checking balances, and conducting business as usual. This resiliency not only prevents service disruptions but also builds customer trust and satisfaction.

3. BaaS with Real-Time Oversight

For sponsor banks offering banking-as-a-service (BaaS), managing fintech relationships requires real-time visibility into funds held on behalf of others (FBO). A digital twin provides the oversight needed to monitor fintech and end-user account balances.

Key benefits include:

- Real-time tracking: Sponsor banks can monitor FBO accounts and fintech balances as transactions occur;
- Simplified reconciliation: Up-to-date data ensures that financial operations and compliance requirements are met efficiently.

This visibility strengthens the bank's position as a reliable partner in the BaaS ecosystem.

4. Seamless M&A Integration

Mergers and acquisitions (M&A) often require banks to consolidate multiple core systems, a process that can be disruptive to customers and fraught with risk.

A digital twin simplifies this challenge by:

- Handling transaction processing independently: Banks can integrate multiple systems without depending on legacy cores;
- Allowing extensive testing: The digital twin can be implemented well in advance of the core switchover, providing time to ensure a smooth migration.

By taking a digital-twin approach, banks can complete M&A transitions confidently, minimizing downtime and ensuring a seamless experience for customers.

FUTURE PROOFING

The digital-twin approach not only addresses today's challenges but also positions banks for future innovation:

- Open Banking: Real-time transaction data stored in the digital twin can be shared with authorized third parties without relying on the core;
- AI Applications: Structured, real-time data from the digital twin supports advanced artificial-intelligence models for fraud detection, predictive analytics, and personalized customer experiences.

Banks no longer need to choose between stability and innovation. The digital-twin approach offers a practical, low-risk solution to modernize banking operations while preserving the reliability of legacy cores.

DISRUPTION PROOFING

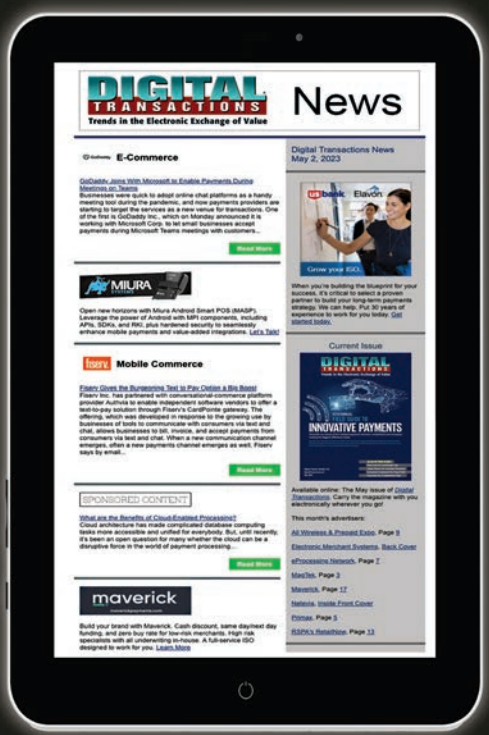
In an era of instant payments and heightened consumer expectations, the digital-twin approach is transforming financial services.

By adopting this innovative technology, banks can unlock real-time capabilities, ensure resiliency, and embrace opportunities in open banking and AI—without the disruption of a core replacement.

As the financial industry evolves, those who leverage the digital twin approach will not only meet the demands of today but also lay the groundwork for the future of banking. 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**

Simplified Security, Maximum Protection

PAYMENTS FOR RESTAURANTS

Magensa Cloud Services offer cutting-edge security for payments, acess, and authentication.

Services

- Magensa Payment Protection Gateway
- Magensa Decrypt and Forward
- Magensa Decrypt
- Magensa TokenExchange

More Ways to Pay

- Apple® Pay and Google® Pay
- PayPal® and Venmo®
- QR Codes and Links
- Hosted Payment Pages
- eCommerce
- Loyalty Tokens
- Subscriptions
- Invoicing
- Swipe, Tap, Dip, Manual, Over the Phone

Learn More About
Magensa
Cloud Services

DynaFlex II Go
with optional charging cradle

DynaFlex II Go

Mobile | Counter | Kiosk

For Secure Payments and Authentication.

MAGTEK®
SECURITY FROM THE INSIDE

Showcasing KwickPOS Solution with MagTek's DynaFlex II Go.

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