DIGITAL TRANSACTIONS

Trends in the Electronic Exchange of Value

18TH ANNUAL

THE 10 MOST PRESSING ISSUES IN E-PAYMENTS

- Merchant Interchange
- Data Breaches
- Antitrust Pressure
- Online Checkout Friction
- AI and Fraud Issues
- Debit Routing Applied to E-Commerce
- Real Time in Retail Payments
- Embedded Payments Reshaping
- Merchant Saturation
- Beneficial Info on Merchants

Volume Twenty-one, Number Eleven • DigitalTransactions.net • November 2024

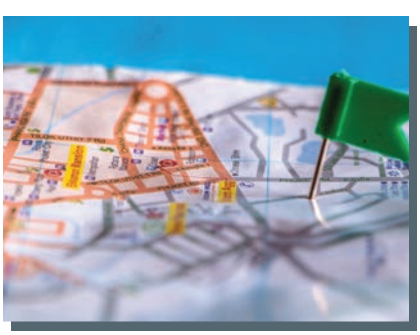
ALSO IN THIS ISSUE:

- Illinois's Interchange Challenge
- Fintechs And Value
- How the ACH Fights Fraud
- Pay By Bank: Safer Than You Think


PAYNETWORX

contents

NOVEMBER 2024 • VOLUME 21, NUMBER 11



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

Magensa Cloud Services Deliver Data Protection to Digital Transactions Wherever They are Made.

Magensa is a PCI-compliant cloud service that enables secure quick response payments (e.g., QR Codes, URL Links, Text-to-Pay, and electronic invoicing) and alternative payments (e.g., digital wallets, PayPal® and Venmo®), with a secure gateway for your payment, access, authentication, and loyalty digital transactions.

- Provide an omni-channel experience for in-person, in-app, unattended, online, and mobile transactions.
- Accept Apple® Pay and Google Pay™ in-app and in-web.
- Deliver Apple VAS® and Google™ SmartTap protocol services like ticketing, loyalty, authentication, and access.
- Enable eCommerce in your payment ecosystem.

Learn More About
Magensa Payment Protection Gateway

NRF2024 RETAIL'S BIG SHOW
JANUARY 14-16 | NYC

SEE YOU AT BOOTH #5375

FIND OUT MORE

562.546.6400
sales@magtek.com
www.magtek.com

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

the gimlet eye

HOW SOON WILL REAL TIME PAYMENTS BE ROUTINE?

HAVE YOU BEEN following developments in the world of faster payments? Probably the most exciting subchapter in this saga is the development and deployment of networks that can deliver real-time transactions, sometimes referred to as instant payments.

But offering the capability for real-time transfers is one thing. Hanging over the payments industry is another question that nobody can answer quite yet, and this is another thing indeed. In a nutshell: With the Federal Reserve's FedNow service having debuted in July last year and The Clearing House Payments Co.'s RTP network in operation since 2017, just how soon can the U.S. payments industry expect widespread, routine exchange of real-time transactions?

Well, answers to that question are beginning to emerge. According to a report released last month by the Faster Payments Council, a trade group, between 70% and 80% of all U.S. financial institutions will be able to receive instant payments by 2028. Ah, but what about sending? On this matter, the report projects between 30% and 40% of financial institutions will have that capability by the same year—a somewhat less robust forecast.

Between late June and mid-August, the FPC surveyed 25 core banking vendors and payment processors for its report, which also documented the use cases most likely to be launched and developed soonest as banks, providers, and users become accustomed to the service. These use cases include earned wage access, domestic peer-to-peer transactions, and wallet funding and defunding. But which real-time applications will prove most popular? The respondents expected earned-wage access, payroll funding, and supplier payments in response to invoices to attract the most real-time adoption.

Other services, however, will take years to be switched on, according to the report. Indeed, if you're hoping for real time in e-commerce and point-of-sale transactions, you're likely to have a long wait. The respondents estimated these applications will require more than four years to be made available.

These survey respondents, by the way, support some 90% of all financial institutions in the U.S. market, according to the FPC. The canvass took place between June and mid-August.

As the report stresses, none of its projections will unfold automatically. Providers will be expected to develop fraud tools that can keep up with the speed of payment, the report stresses by way of example. Other needs involve improved error resolution and suitable user interfaces, not to mention technology such as QR codes for that far-off point-of-sale adoption. Then there's the tech required for request for payment and APIs to ease deployment and adoption.

The research effort gives us a glimpse of what the industry can expect. We'll soon see if reality matches up.

John Stewart, Editor | john@digitaltransactions.net

NOVEMBER 2024 • VOL. 21, NO. 11

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.

HOW ILLINOIS'S INTERCHANGE CASE HAS TRANSFIXED THE INDUSTRY

Plaintiffs in a lawsuit seeking to overturn the Illinois Interchange Fee Prohibition Act filed motions last month requesting the court deny a request from several merchant organizations to join the Illinois Attorney General as defendants in the suit.

The case, which involves a recent Illinois law that prohibits interchange on the tax and tip portion of card transactions, has roiled the payments industry nationwide for months ("The Prairie State's National Challenge," September). At the heart of the plaintiffs' argument is that the Illinois Attorney General is not only "actively defending" the Illinois Interchange Fee Prohibition Act (IIFPA), but also that retail associations "do not propose to add anything to the merits of the case because their legal arguments mirror those of the Attorney General."

Plaintiffs in the case—generally, those who oppose the law's interchange exemption for tips and tax—are working to prevent it from taking effect July 1, 2025, as scheduled by the legislation. Meanwhile, the case has inspired a whirlwind of motions from both proponents and opponents. A ruling from the court was expected Oct. 30, after this issue of *Digital Transactions* went to press.

The Illinois Retail Merchants Association, the Illinois Fuel and Retail Association, the National Association of Convenience Stores, the National Retail Federation, and FMI, the food-industry association, are the merchant groups that this fall filed a request to intervene in the case as defendants.

The groups requested to join the suit because they feel they could provide the court with more facts and insights about how the payments system works. The move is part of an effort to refute plaintiffs' claims that the law will negatively disrupt the payments system, according to Doug Kantor, general counsel for the National Association of Convenience Stores.

To further their argument against the intervention, the plaintiffs contend their challenge to the legality of the IIFPA is a question the Illinois "Attorney General is fully competent to litigate."

In contrast, they add that the retail associations' intervention in the case "would only add distraction and complexity by using party status as a staging ground for their policy interests."

The Illinois Bankers Association, The American Bankers Association, the Illinois Credit Union League, and America's Credit Unions, formerly the National Association of Federally-

Insured Credit Unions in August filed the lawsuit challenging the IIFPA.

While the IIFPA exempts Illinois merchants from paying interchange on sales tax and gratuities linked to credit and debit card transactions, the state will cap what merchants earn for collecting sales tax at $1,000 per month.

The plaintiff's motion also argues that as a "governmental body charged by law with protecting the interests of the proposed intervenors," the Illinois Attorney General "is presumed to adequately represent" the merchant organizations' interests "unless there is a showing of gross negligence or bad faith" on the part of that office.

Finally, the plaintiffs contend that any "perspective" from the retailer organizations could be shared in an amicus brief "without unduly burdening the court and prejudicing plaintiffs."

The plaintiffs note that other parties, such as the Office of the Comptroller of the Currency, a federal agency "with relevant authority and expertise" in payment systems, have filed amicus briefs arguing against the legality of the IIFPA without requesting to intervene in the case. The OCC filed an amicus brief earlier this month opposing the law and supporting the plaintiff's request for an injunction.

Plaintiffs add they have no objection to the merchant organizations filing an amicus brief to make their arguments for the IIFPA.

Merchant organizations viewed the latest motion filed by the plaintiffs as a sign the law's opponents are concerned about the merits of their case. "It's not surprising that [the plaintiffs] are concerned the court might learn the truth from the merchant organizations seeking to intervene in the case," Kantor says.

In addition to filing a motion urging the court to deny the intervention request, the plaintiffs filed another motion last month arguing against the Illinois Attorney General's request to deny a preliminary injunction against the IIFPA.

In that motion, the plaintiffs argue that, if allowed to take effect, IIFPA "would require banks, savings banks, credit unions, and networks worldwide to overhaul payments systems that allow consumers and merchants to instantly consummate millions of transactions every day."

Plaintiffs also restated their argument that the IIFPA "is pre-empted under multiple sources of federal law and, in turn, invalid under state and federal law that guarantee state-chartered institutions competitive parity."

Granting a preliminary injunction, plaintiffs argue, would cost "millions of dollars' investment in new automated systems" and would involve "mindbogglingly burdensome manual processes" that will be wasted when the law "is eventually found invalid."

The Illinois Attorney General's Office says it does not comment on pending litigation.

—Peter Lucas

'THE DAYS OF EASY SECULAR GROWTH ARE BEHIND US," WARNS A NEW REPORT

Payments revenue, which grew at a healthy clip through last year, is going to see a drastically slower growth rate over the next five years, argues the Boston Consulting Group in a report issued mid-October.

Worldwide payments revenues, which totaled $1.8 trillion last year, will increase at a compound annual rate of 5% over the five years through 2028, argues the report, entitled "Fortune Favors the Bold." While that rate of growth will yield a $2.3 trillion market by then, it is notably down from the 9% CAGR the global industry generated in the five years through 2023, the report says.

The story in the North American market is little different, with the industry tapping the brakes to the extent that growth in payments revenue will slow to little more than 3% in the next five years. That's a slide from the nearly 10% rate in the half decade through last year and represents one of the most dramatic drops among regions worldwide, the report warns.

Transaction revenue includes earnings from card and non-card payment instruments, according to the report.

Part of the slowdown can be attributed to the near-complete conversion of cash to digital payments, the report notes. In markets like the

United States, the United Kingdom, and the Nordic countries, less than 10% of transactions by value are now conducted in cash, BCG says.

"The payments industry is entering a new phase, and the days of easy secular growth are behind us," warns Inderpreet Batra, managing director and senior partner at BCG and a coauthor of the report, in a statement released with the report.

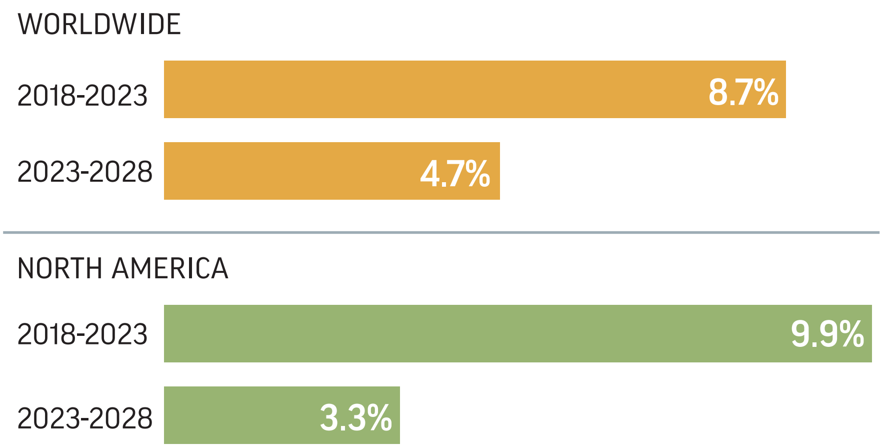
To re-energize growth, he says, banks and payments companies will have to install and use newer technologies, including generative artificial intelligence, and also stop the bleeding from fraud by beefing up risk and compliance technology.

While BCG is predicting a significant slowdown in revenue growth, it also recommends that banks and other payments players pay close attention to developments in real-time payments, including central bank digital currencies. These trends, it says, offer new revenue opportunities but also new costs and other challenges. That means payments companies will be best positioned to benefit from the new technologies if they "act decisively now" in adopting them, notes Markus Ampenberg, a managing partner and partner at BCG, in a statement.

—John Stewart

NORTH AMERICA HITS THE BRAKES

(Transaction revenue growth rate, actual and projected)



Source: Boston Consulting Group

HOW VISA AND SWIFT ARE PLUNGING DEEPER INTO DIGITAL CURRENCIES

Payments companies may not yet be ready to embrace fully the world of blockchains, but some major payments networks are taking steps to deepen their experience in that world. Witness Visa Inc., which last month said it will help banks issue tokens they create on a blockchain. The tokens will be backed by fiat money, such as dollars.

So-called live pilots for the service, dubbed VTAP for Visa Tokenized Asset Platform, are expected to start next year, Visa says, with BBVA as the participating bank.

The news comes at the same time as an announcement from Swift, the Brussels-based international financial-messaging network, that it intends to run what it calls trial transactions with digital currencies and assets. As with Visa's initiative, the Swift project is expected to start in 2025.

VTAP, which Visa says has been developed internally by "blockchain experts," is aimed at least initially at business-to-business transactions. It's also intended to make it easier for banks to introduce fiat currencies into blockchain systems, Visa says.

The new platform has what Visa says are three major advantages. One is ease of access to the Visa platform. Participating banks, for example, can create an integration to the platform using application programming interfaces.

A second advantage is what the network calls programmability, which will allow banks to use so-called smart contracts to control the issuance of payments when prearranged terms are met. The third benefit, Visa says, is that VTAP will offer interoperability across multiple blockchains through a single application programming interface.

BBVA has been testing the system this year, according to Visa, and intends to launch what the network calls a "live pilot" next year on the Ethereum blockchain. "This collaboration marks a significant milestone in our exploration of the potential of blockchain technology and will ultimately help enable us to broaden our banking services and expand the market with new financial solutions," said Francisco Maroto, head of blockchain and digital assets at BBVA, in a statement.

Visa is not new to the world of blockchain-based currencies. A year ago, for example, it announced a pilot to extend its cryptocurrency services into merchant acquiring for cross-border transactions. That initiative included support from the major processors Worldpay and Nuvei, as well as processing on the Ethereum and Solana blockchains.

Meanwhile, Swift said it has already run transactions using tokenized value through both public and private blockchains. Now, the network wants to test ways it could provide what it calls "a single window of access to multiple digital-asset classes and currencies."

The network says its initiative will start with payments as well as foreign exchange, securities, and trade. Its goal, it says, is to be the connecting facility for isolated "digital islands" whose disparate standards prevent ready-made interconnection.

"With Swift's vast global reach, we are uniquely positioned to bridge both emerging and established forms of value, and we're now focused on demonstrating this in real-world, mainstream applications." said Tom Zschach, Swift's chief innovation officer, in a statement.

Swift, which was founded in 1973 and went live four years later, says its platform links more than 11,500 banks, securities firms, corporate customers, and "market infrastructures" in more than 200 countries and territories.

—John Stewart

BATTLING FRAUD: AI'S LOOMING ROLE AND TRULIOO'S NEW ANTI-FRAUD TOOL

With just days until the traditional start of the holiday shopping season post-Thanksgiving, consumers and criminals alike are gearing up for a busy period. A new report from ACI Worldwide Inc. forecasts that synthetic-identity fraud and artificial intelligence will amount to a big lump of coal for merchants.

Meanwhile, the identity platform Trulioo recently debuted a new tool to help merchants counter synthetic and third-party fraud.

ACI, in its annual "Unwrapping Checkout Trends" report, says its data show fraud increased 3% in the first half of 2024 year-over-year, with synthetic identity fraud growing 26% in the period. Synthetic identity fraud refers to cases where criminals merge genuine information with fabricated data to create an identity that may appear authentic and can be used to open accounts and make fraudulent purchases, ACI says.

This holiday shopping season, ACI forecasts that criminals will increase their use of AI tools to exploit vulnerabilities and mask their activities with fake accounts and identities, all the better to scale their attacks. While automated bots have long been a component of fraud, the introduction of easier-to-use AI technology makes the threat more powerful.

"[Since] at least a year back we've been seeing a rapid growth in industrialized AI impersonation. The burst-like growth can be accounted to fraudsters' success in implementing randomization into GAI ID (generative artificial intelligence) documents and biometrics. This enabled the mass-production of potentially never-repeating documents and biometrics," Ofer Friedman, chief business development officer for AU10TIX, told *Digital Transactions News* in September.

ACI suggests merchants should also use AI tools to help deal with the threat. "The rapid proliferation of AI-driven fraud tactics and stolen data on the dark Web is escalating threats, making it harder than ever for merchants to distinguish real customers," Cleber Martins, ACI head of payments intelligence and risk solutions, said in a statement.

"Merchants should tighten their defenses by harnessing AI predictive modeling to detect threats and using payment-intelligence signals to eliminate false positives without disrupting genuine transactions," he continued.

ACI forecasts holiday-shopping transaction volumes will increase 3% on Thanksgiving and 4% on the Friday after it—known as Black Friday—compared with 2023 levels. The most growth is predicted for Cyber Monday, the Monday after Thanksgiving, with an expected 12% increase.

In related news, Vancouver, British Columbia-based Trulioo last month released its Trulioo Fraud Intelligence service, which the company says can provide predictive transaction insights across more than 195 countries.

Among its features are a single integrated platform that includes know-your-customer data checks, identity document verification, watchlist screening, and fraud intelligence, all Trulioo-branded services. It also provides a consolidated risk score and global data sets to help tune risk models to each country, according to the company.

—Kevin Woodward

MONTHLY MERCHANT METRIC

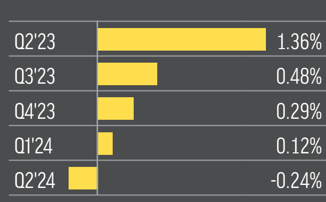
Total Same Store Sales YOY Growth %

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 merchants defined as merchants with **less than $5M in annual card volume.**

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

Same Store Sales YOY Growth % - Annual volume change/growth of retained (non-attrited merchants with positive revenue and volume)



Note: Previous metric included all active merchants, those with positive revenue, whereas the new metric shown only includes merchants with postive revenue and volume.

payarc

Overhaul Your Payment Processing with Payarc's PAYFAC Platform

Empower Your Business with Seamless Transactions

In today's digital ecosystem, software companies have a wide range of options to create unique payment experience for consumers. Recently, payment facilitation has been an increasingly popular choice for business owners when it comes to accepting payments. Instead of each business needing to establish its own merchant account, the PAYFAC provider has a master account and sub-accounts for all their clients, allowing inquiring businesses to onboard quickly and efficiently.

At Payarc, our PAYFAC Platform is designed to **simplify the process of managing payments for established software platforms and their users.** By offering unique advantages and features to streamline the overall process, we have distanced ourselves from the competition.

Why Payarc?

Seamless Integration
- Streamline business operations by integrating with accounting, inventory management, and CRM platforms.
- Enhance efficiency and focus on business growth

Omnichannel Solutions
- Provide a seamless payment experience across online, in-store, and mobile channels.
- Empower merchants with flexible processing through proprietary apps and gateways.

White Glove Support and One Call Resolution
- Access personalized assistance with one-call resolutions
- Enjoy 24/7 support with our dedicated team answering your calls within 45 seconds.

Your Success, Our Commitment

At Payarc, success is not just a goal; it's a commitment. We provide comprehensive tools and support for all your payment facilitation needs, from our user-friendly dashboard to splitting payments, onboarding, payment integration, and more. With our white-glove support team. We'll make sure every aspect of your business is covered quickly and efficiently.

API Integration Capabilities for Traditional and PAYFAC Models

Did you know that Payarc offers seamless API integration for both traditional merchant processing and payment facilitation models? Whether you are looking to streamline traditional processing with robust onboarding or leverage the speed and flexibility of payment facilitation, our solutions are designed to enhance your payment experience.

Explore how these options can impact your business, from merchant sign-ups to payment timeline and billing choices. Get in contact with us to understand the key differences and discover which model best suits your business' needs.

Why Choose our PAYFAC Platform

Dashboard Excellence
- Every ISV sub-merchant is assigned a unique ID in the Payarc system.
- The central dashboard is a hub of powerful tools to efficiently manage daily tasks - from reconciling transactions, handling chargebacks, and more.

Split Payments
- Gain control of funding instructions with our Split Payments API or Virtual Terminal.
- Divide your transactions into smaller accounts or accounts that do not process transactions.

Payment Integration Options
- Select the onboarding option that aligns with your preferences within the program.
- Real-time automated underwriting checks with in-house developed UI or API integrations.

ID Provisioning / Onboarding
- Select the onboarding option that aligns with your preferences within the program.
- Real-time automated underwriting checks with in-house developed UI or API integrations.

Electronic Payment Acceptance Variety
- Multitude of options for accepting electronic payments like cards, ACH transactions, virtual terminals, invoices, dual pricing, and more.
- Tailor your payment plan to align with every need to surpass customer expectations.

See you next year!

WSAA
SEAA SOUTHEAST ACQUIRERS ASSOCIATION
MWAA MIDWEST ACQUIRERS ASSOCIATION
TRANSACT POWERED BY ETA
Retail NOW
SaaStr ANNUAL

www.payarc.com 1 (877) 203-6624 sales@payarc.com

payarc

LOANCHAIN: A NEW MARKET FOR ENTREPRENEURS

BY
GIDEON SAMID
gideon@bitmint.com

BLOCKCHAIN IS ROBBING traditional banks. It's yanking money from beyond concrete walls, metal locks, and private ledgers and putting it behind cryptographic walls, mathematical locks, and public ledgers. As legacy banks gasp for air, here comes the one-two-punch: LoanChain.

Its blow may be deeper at the core level. Banks make their money on the gap between the interest they charge borrowers and the interest they pay depositors. Banks flourish because they present themselves as the only safe place for money held by the public, so depositors are happy with the security and keep hundreds of billions of dollars deposited without claiming any interest, or minimal interest.

This abuse of depositors is waiting for a Robin Hood: LoanChain. It's following its predecessor, blockchain. Blockchain is based on public visibility of all digital accounts, with cryptographic blindness as to the identity of the account holders. LoanChain is based on public visibility of traders wishing to borrow money combined with visibility of traders who wish to lend money.

As things are now, there is a mismatch. Borrowers vie for large loans for extended periods of time, while lenders would prefer to risk a low sum and get the money back quickly. LoanChain resolves this mismatch by constructing a chain, serving a year-long loan with a succession of short-terms lenders. And on occasion, a single large-sum, long-range lender will be served by a chain of smaller-sum, shorter-range borrowers.

The chain of lenders passes the money from each lender to its predecessor, getting its money back from its successor. Meanwhile, borrowers have no idea that a chain of lenders is serving them. A loan of $1 million extended for a year can be served by 100 chains of $10,000 each, where each chain comprises 52 ledgers, each one week long.

LoanChain relies on instant payment protocols, like BitMint, where the transacted money is never in a state of ambiguity. At any instant, the money is either in the hands of the payor or in the hands of the payee. LoanChain involves a gusher of money movements all across cyberspace. Supply and demand are on naked display, dynamically moving the interest the borrower pays, the interest the lenders receive, and the profit of the LoanChain entrepreneur.

No money moves if there is no match between lender and borrower. No overhead, no elaborate long-term saving accounts, no money markets or similar drag.

Administering LoanChain is cyber-centric, with no branches and no sales gimmicks. In fact, t he digital realm offers staggering flexibility. You close business at 6 p.m. You don't need your money before 8 a.m. the next day, so the LoanChain app is lending your money while you sleep. The funds are back at your disposal when you need them the next day. And legacy banks are nowhere near the action.

Using BitMint's digital claim-check technology LoanChain establishes cash-ready collateral to mitigate the risk of failed loans. And borrowers will be building their credit rating by starting with small, short-range loans, paying them off and climbing further.

Much as with blockchain, the LoanChain solution will be offered to the public by competing entrepreneurs. Eventually, banks will be joining in. If the regulatory climate allows it, lenders will remain private, but no less eager. LoanChain's efficiency stems from its global visibility and the fact that no deposit is accepted unless a borrower takes the money.

Digital money is paid through the devices belonging to the payors and the payees. In turn, the devices follow policy set up by a human agent. Execution involves AI optimization. Query the author for details.

Blockchain, Loanchain—what's next? DT

FOR AI, HAVE A STRATEGY FIRST

BY BEN JACKSON

bjackson@pa.org

SUCCESS WITH ARTIFICIAL intelligence is about strategy, but most conversations about AI today focus on tactics.

Although financial services have used AI for decades, the growth of generative AI has led to a broader set of use cases. Innovators are looking for ways to apply artificial intelligence to everything from customer service to regulatory compliance.

While each of these tools can be valuable, the greatest success will come to those companies that use AI for strategic goals.

Last month, I attended the AI-Native Banking and Fintech conference organized by Spring Labs, an AI company focused on customer support and compliance. The sessions focused on AI for functions like customer service and process automation, along with discussions on the regulatory implications of using AI.

In one panel, Jordan Wright, the chief executive and co-founder of Atomic, a company focused on API account connections, bridged the discussion from tactical to strategic. He described how his company uses AI for things like developing sales pitches and offering account-management tools.

Wright said he hoped AI would enable Atomic to grow to a $1-billion company, with the 20 employees it has, by helping it offer additional products and services while operating efficiently. This framing shows how AI can apply to a larger strategy. While AI can spot fraud, reduce costs, or simplify document reviews, no company will have a monopoly on it.

Companies must plan how to differentiate themselves when all their competitors also have chatbots for customer service, machine learning for identifying fraud, and generative AI for marketing.

Margaret Mayer, chief technology officer at Zions Bank, predicted that, over the next year, banks will see incremental gains from AI. But in five years, she said, AI will transform the industry. She said her bank is preparing by having a data-science team and an internal sandbox to test products.

Still, she worried about the risks posed by AI. One concern she cited was how well customers would understand what they are consenting to when they give permissions for systems to access data, particularly in an open-banking environment.

A second concern Mayer and others raised: How regulators might react to AI-driven changes in the industry.

One answer is that banks are already prepared to deal with regulatory risks. Anne Romatowski, a markets-program manager for the Consumer Financial Protection Bureau, pointed out that current laws do not change just because there is new technology.

Similarly, customers' core needs do not change just because the technology to meet those needs has changed. They still need to make payments, save money, borrow money, and manage their financial lives. Companies will need to keep customer needs centered as they begin to integrate new tools.

An additional strategic consideration companies will need to consider is that two things limit the power of AI tools: the robustness of the models and the quality of data used to train those models.

As Derek Higginbotham, president and chief executive of First Electronic Bank pointed out, the models can drift over time based on the data they receive, and that can lead to problems if management is not paying attention.

The second risk is the "black swan" event that fits a model or its training data set but turns a portfolio upside down. Companies will need to think holistically so they know when to adjust a model, or even go against an AI system's recommendation in response to novel market conditions.

All of this requires that a company's leadership knows what its core business is and what its core strategy is. Without that, AI is just a tool to manage a bureaucracy. DT

IN TODAY'S FINTECH MARKET, VALUE IS EVERYTHING

Payments providers and related technology firms can follow a detailed roadmap for success, regardless of the level of competition.

BY **JEFF WOOD**

Jeff Wood is principal at the Alexander Group.

BETWEEN THE DEVELOPMENT of new technologies and the proliferation of providers, today's fintech market is as competitive as it's ever been. Indeed, the industry has shown signs of an upswing. The first quarter of 2024 saw more M&A activity than we've seen in more than two years, a sign that coffers are full and businesses are hungry to make strategic investments.

Fintech companies face a whole host of imperatives to succeed in an industry abuzz with excitement. These imperatives include enhancing their value proposition, standing out from the crowd, growing profitable revenue, protecting margins, and retaining existing customers. How can they get it all done?

It all comes down to value-added services. Fintech firms should thoughtfully explore ways to introduce add-on offerings to existing accounts. At the same time, they must consider how sales, marketing, account management, and customer success come into play, as well as the resulting impact on sales compensation. In doing so, organizations can unlock cross- and upsell opportunities, provide superior customer experience, and drive enhanced productivity.

This article explores best practices for any fintech company looking to protect and expand its market share to drive profitable growth.

WHAT ARE VALUE-ADDED SERVICES?

To put it plainly, value-added services are those that extend beyond the core offering to deliver additional value. For fintech organizations, these add-ons might include e-commerce support, loyalty programs, affiliate marketing, or cross-border payments.

Value-added services are key because they open the door for more business. Whether through upsell opportunities like user-base expansions, increased consumption, and term extensions or through cross-sell plays like product launches, value-added services can make all the difference for organizations hoping to build lasting success.

Sales teams have an instrumental role in a company's strategy here. By showing customers all the capabilities their organization has to offer, sales reps can help evolve their firm's positioning from a point solution—marked by singular or disparate services—to a platform play, featuring a comprehensive breadth of interconnected services. Platform structures help fintech leaders kill three birds with one stone: drive higher net revenue retention (NRR), grow market share, and retain existing business.

As leaders look to offer value-added services, they need executive alignment on which specific services should be prioritized. Then, they must align go-to-market (GTM) execution based on the priority and development stage of each of the new offerings. Leaders might consider questions like these:

- Which add-ons are more mature and will be core to our GTM strategy?
- Which offerings require building buyer awareness with a first wave of customers?
- What best aligns with our company's growth plan?
- What will position us most advantageously?

Firms must assess the market readiness of any proposed value-added service before moving forward.

Once the specific value-adds have been selected, it's time to integrate them into the GTM strategy. Next steps include documenting use cases, outlining the buyer journey, building an expansion pipeline, and integrating with formal customer-success initiatives.

COVERAGE AND JOB ROLES

With a clear strategic priority and goals set for value-added services, leaders must align the GTM coverage model and rules of engagement across roles to ensure successful execution of the strategy.

Fintech firms must determine who will serve as primary point person to drive the new services, both to existing clients and new logos: a core rep or a specialist rep.

- **Core reps** were likely responsible for winning the account and selling the flagship offering. They tend to know the client best and have a very strong rapport. They possess excellent generalist knowledge of the firm's primary offerings, including up- and cross-sell opportunities.
- **Specialist reps** have—it might go without saying—specialized knowledge beyond the capacity of the core rep. They can dive into the weeds to serve as the expert on a specific value-added offering. They might have joined the firm during an acquisition, or they might have been engaged when the value-added service was first launched.

It's imperative for fintech leaders to work with their teams to determine the best arrangement for each segment, region, or use case to pursue as a priority. The GTM coverage model and buyer journey must be tailored carefully based on whether a core rep, specialist rep, or combination will be involved.

If both a core and a specialist rep are serving an account, they need a playbook and formal rules of engagement that specify respective responsibilities and customer touchpoints. Who handles pre- versus post-sales motions? Who handles day-to-day communication? Often, the core rep is well-suited to serve as a quarterback in these arrangements, but this might not always be best. What's most important is that the core and specialist reps are in symbiotic lockstep to keep the account running smoothly.

For these arrangements to be successful, compensation structures must also be determined to maintain alignment with the team's desired behavior.

SALES COMPENSATION DRIVES PRODUCTIVITY

There are several ways to leverage compensation as an incentive to drive focus on value-added services. Answering some key questions at the onset can help steer organizations toward the compensation lever that will drive maximum productivity among their reps.

- Is there a clear consensus within the organization on the importance of selling and promoting value-added services?
- Where is the value-added service in the product lifecycle management process?
- Is it mandatory or optional for core reps to sell value-added services?
- Can the organization set an accurate quota for value-added services?
- How much is the organization willing to invest in compensation toward value-added services?

Firms that wish to offer even more incentives for selling value-added services can use a credit-value adjustment, a rate-value adjustment, or an add-on bonus—but they must be sure of the budget for doing so. Penalties such as hurdles may be put in place to further encourage meeting these quotas.

Fintech leaders must be sure their compensation plan changes will drive the desired behavior among sellers. Organizations must thread the needle so their compensation plans are sufficiently motivating while still falling within the guidelines of the company's cost model.

AI HAS A ROLE TO PLAY, TOO.

Artificial intelligence (AI) and machine learning (ML) can help fintech firms get up and running with value-added services, as well. AI/ML can comb through troves of data to help fintech firms identify priority expansion use cases and sales plays for value-added services. This analysis allows organizations to easily and effectively grow in ways that make the most sense for themselves and their customers.

AI can also be used to optimize forecasting and quota setting, resulting in compensation plans that are more data-driven and successful.

VALUE-ADDED SERVICES ARE KEY TO DIFFERENTIATION.

Fintech companies that effectively incorporate value-added services into their GTM strategies will ultimately strengthen their relationship with clients, enjoy enhanced competitive differentiation, and achieve stronger profitable growth.

By focusing on applying the right coverage model and compensation plans, fintech firms can ensure any new or enhanced offerings are launched smoothly. Prioritizing value-added services as key components of sales teams will help organizations drive long-term success. DT

Wood

Wood: Fintech companies face a whole host of imperatives to succeed in an industry abuzz with excitement.

BAD ACTORS AND THE AUTOMATED CLEARING HOUSE

While ACH fraud is persistent, so too are efforts to thwart criminals intending to disrupt legitimate payments.

BY KEVIN WOODWARD

IMPOSTERS, ACCOUNT takeovers, and phishing cause a lot of payments headaches, and in this respect the automated clearing house channel is no different. Criminals even adapt familiar check-kiting schemes—which rely on float to reap ill-gotten gains—to take advantage of the transaction time when moving funds from one account to another with a conventional ACH payment.

ACH fraud may not garner tons of attention. as do some other fraud categories, but that doesn't mean there isn't plenty of it. Criminals have shown themselves to be intent on manipulating ACH transactions to their advantage.

In 2023, according to the 2024 AFP Payments Fraud and Control Survey Report, 33% of organizations said ACH fraud was a problem, up from 30% in 2022, based on 521 responses to the Association for Financial Professionals survey.

To put that in context, the same report found 65% of organizations were affected by check fraud in 2023.

"Every payment system has to deal with fraud," says Michael Herd, executive vice president of ACH network administration at Nacha, the automated clearing house rulemaker. He points to a 2023 Federal Reserve survey of financial-institution risk officers that showed 22% were experiencing attempted ACH fraud, compared with 52% that sustained check fraud.

'SOPHISTICATED TACTICS'

Still, ACH fraud is an issue. Fraud types involve creating new, fraudulent accounts online, says Yinglian Xie, chief executive and founder of Datavisor Inc., a Mountain View, Calif.-based fraud and risk platform.

"Fraudsters use a variety of sophisticated tactics to commit ACH fraud, exploiting the system in increasingly sneaky and complex ways," Xie says. "One trend we've observed is a notable increase in ACH kiting, where fraudsters employ interconnected and intertwined attack tactics. These perpetrators use multiple strategies simultaneously to execute their fraudulent schemes"

"One rising tactic involves creating new, fraudulent accounts online," Xie continues. "Fraudsters enroll in online banking and transfer funds from external accounts to these newly opened accounts. They then exploit the time delay in ACH transactions, swiftly withdrawing the funds before any unpaid ACH debits are detected."

"Additionally, fraudsters leverage compromised accounts to conduct similar fraudulent activities," she says. "By accessing these accounts, they transfer funds from external sources into the compromised accounts and

THE ACH: A 10-YEAR PERSPECTIVE

(Results 2014 through 2023)

Payments	4.8%
Dollar Volume	4.4%
Total Payments	31.45 BILLION
Debits	17.74 BILLION
Credits	13.71 BILLION
Total Dollars Transferred	$80.1 TRILLION

Source: Nacha

Herd

Herd: New Nacha rules "will require all participants in the ACH Network to conduct base-level monitoring of their ACH payment activity."

withdraw the funds before any unpaid ACH debits are identified."

Other types of ACH fraud involve payroll. The latest Nacha data show second-quarter 2024 direct-deposit transactions at 2.1 billion, though not all may be payroll transactions—one of the largest uses of the ACH network, says Tom Randklev, head of product at London-based CellPoint Digital, a payments-orchestration provider. Phishing and data breaches are other significant factors affecting ACH fraud, Randklev says.

Fraudulent ACH return fraud is yet another concern, says Nathan Hilt, managing director at Protiviti Inc., a Menlo Park, Calif.-based consulting firm. In these instances, consumer debits have an extended return timeframe of 60 calendar days from settlement and can be returned as unauthorized by the consumer, he says.

"In the case of legitimate fraud, the consumer is granted this protection as an added benefit, but we also see bad actors knowingly return the entry as unauthorized," Hilt says.

There's also ghost funding, which "typically occurs when the customer is granted immediate access to funds which have not yet settled fully across the ACH network," Hilt says.

"Typically," he says, "we see this used with investment accounts where funds are immediately credited. When the funds come back [insufficient funds] there is no ability to recover the funds because the fraudster has either transferred the money to another account or used it to purchase an unrecoverable asset like crypto."

STAYING IN CONTACT

Business email compromise can be yet another gateway to ACH fraud. In 2023, according to the AFP report, 38% of organizations said they experienced this fraud. Generally, these email compromises can appear to be from a known source, making the request look more legitimate, the FBI says in a post about the fraud.

A scammer might spoof an email account or Web site. They could use malware or send a spearphishing email, which appears to be from a trusted sender, to trick victims into revealing confidential information.

Nacha, as the chief rulemaker for the ACH network, is well aware of how criminals could use the system to capitalize on opportunities.

Herndon, Va.-based Nacha says it has new rules to address credit-push fraud. "The rules will require all participants in the ACH Network to conduct base-level monitoring of their ACH payment activity," Herd says. "This requirement covers the financial institutions receiving the payments, acknowledging that these institutions might be in the best position to identify questionable payments being received to accounts within their institutions."

> Xie: Fraudsters are "exploiting the system in increasingly sneaky and complex ways."

Under these new rules, "all participants in the ACH network, except consumers, will conduct a base-level of fraud monitoring on ACH payments, including ACH credits," Jane Larimer, Nacha president and chief executive, wrote when the rules were announced in March.

Herd says Nacha puts its network to use to help members contact one another, a service called the ACH Contact Registry, to help financial institutions connect with other participants in instances of fraud or questionable payments.

"Interestingly, the ACH Contact Registry is also the industry's largest source of contact information for personnel responsible for check payments, so it is helpful to institutions in addressing instances of check fraud," Herd says.

'REALLY DIFFICULT'

Even beyond rules already in place, organizations can do a lot to stymie ACH fraud. Xie suggests prioritizing three elements. "First, they must closely monitor customer and ACH transaction behaviors," she says. "Vigilance in detecting irregularities in transaction patterns, such as out-of-pattern behavior or the addition of new, previously unassociated recipients with significant amounts, is crucial.

"By taking a customer-centric approach and analyzing all customer behaviors and transactions, not just ACH transactions, organizations can enhance their ability to identify potential risks," she adds.

Another element is to incorporate technology that can illuminate the social relationships between ACH transfer senders and recipients, Xie says. "Implementing intelligent methods to identify connections, such as name and address similarities, and leveraging historical transfer activities and other payment histories, can uncover potential fraud," she says.

"Lastly, prioritizing a comprehensive identity-verification process is essential. Robust identity-verification protocols help establish a solid foundation for detecting and mitigating fraudulent ACH transactions," says Xie.

A key component to reducing ACH fraud is educating users, whether they are businesses or consumers. Both sets of users can fall victim to nefarious schemes, such as phishing. "With phishing fraud, you have to rely [on the idea] that your customers are educated," Siva Narendra, chief executive and founder of Tyfone Inc., a digital banking and payments provider, tells *Digital Transactions*. "That's really difficult."

That's because, in part, large language models, often used in artificial intelligence, are being used by criminals. "You no longer get this 'prince of Nigeria' email, it's highly sophisticated emails," Narendra says. The "prince of Nigeria" phishing emails are a type of advance-fee fraud.

Education is part of a multilayered approach and should include employee education, too, says Kimberly Sutherland, LexisNexis Risk Solutions vice president of fraud and identity management strategy.

"Because people are seeing this activity at work, they carry these learned behaviors on how to avoid phishing scams and increase their awareness of the need for authentication," Sutherland tells *Digital Transactions*.

Even with measures in place and updated rules to ensure sending and receiving institutions are equipped to counter ACH fraud, criminals are still going to target ACH transfers until these transactions are no longer profitable for them.

"ACH fraud will exist as long as ACH transactions occur," Sutherland says. Because ACH is a popular payment option, and because it's very affordable for businesses to use, ACH transfers will increase. That may only change when alternatives that offer the same level of affordability and relatively low risk emerge. Still, criminals are going to following the activity, Sutherland says, adding, "Fraud is something that is going to be around." DT

> Hilt: Ghost funding "typically occurs when the customer is granted immediate access to funds which have not yet settled fully across the ACH network."

18TH ANNUAL

THE 10 MOST PRESSING ISSUES IN E-PAYMENTS

We know you’re not looking for problems. But they are looking for you. Herewith our annual catalog of the ones causing the most headaches.

BY PETER LUCAS, JOHN STEWART, AND KEVIN WOODWARD

EACH YEAR IN THE FALL, as the grass turns brown and the trees shed their leaves, the editors of Digital Transactions start their deliberations over an equally gray and shadowy subject: what's cramping the style of payments players these days? What obstacles are they confronting, and how? Which ones are pressing harder than the others, and why?

If adversity breeds strength, as the old saying goes, then payments professionals these days may have plenty of opportunity to develop their strategic and tactical biceps. The industry no sooner recovered from all the ill effects of the pandemic than it found itself enmeshed in a slew of other issues, some old and familiar but some others quite surprisingly fresh.

Herewith our annual catalog of the problems we think are most alarming for payments professionals right now, ranked in order of their impact—or potential impact—on the industry. "Impact," of course, can be a matter of degree. Some of the matters ranked below, however, may be no less pressing for being still more or less in their larval stage.

So, what do we mean by "pressing"? The term refers to the sense of urgency the issue arouses in those it affects, not so much to the size of the market that must deal with it. Some issues, on the other hand, are pressing for a substantial segment of the industry.

Take our number-one issue this year, merchant interchange. There's nothing new about this issue. Card-accepting merchants have griped about acceptance costs for decades. It has inspired lawsuits and legislation, as well as a good deal of animosity toward banks and allied entities. Yet never has the issue been hotter than it is now. For that reason alone, it has climbed to the number-one spot in this year's ranking.

Speaking of the ranking, it was done by our staff editors, who cover this industry day by day. You may agree or disagree. Either way, let us know what you think the big issues in payments are, and we'll take up the matter with our 19th annual ranking next year. Meanwhile, you can reach me with your comments at john@digitaltransactions.net.

1 Merchant Interchange

It's hard to think of an issue in digital payments more contentious than interchange. The subject can be complicated, but it essentially refers to the fee merchants pay to acquiring banks whenever they accept a card for payment. The fee is typically expressed as a percentage of the transaction amount, plus a dime or two. So a $100 card transaction might cost the seller in the neighborhood of $2 or $3.

So the merchant in this case gets $98 or $97 on the $100 transaction, and walks away pretty sore. Acquirers, on the other hand, point to the services they provide—including processing connections and transaction guarantees—as justification for the fee.

The latest example of the contentious nature of this issue has emerged in Illinois, where lawmakers passed a bill earlier this year exempting the tax and tip portion of a bill from interchange calculations. In return, the law limits what merchants can earn from the state for collecting sales tax at $1,000 per month. The Illinois Interchange Prohibition Act has attracted national attention as card interests sue to overturn it and merchant groups battle to keep it in place.

In any case, what happens in Illinois is not likely to stay there. Interest groups on both sides are filing briefs in the case and watching closely, while merchant groups hope to duplicate the law in other states and perhaps nationwide. Ultimately, merchants would like to see interchange rates themselves controlled nationally, something another piece of legislation, the Credit Card Competition Act, proposes to do by requiring more competition among networks for each transaction. This bill, which has languished in Congress since it emerged two years ago, has stoked furious advocacy among merchants and equally stalwart opposition from interest groups representing banks.

Whatever happens, the ancient dispute over interchange only grows more heated, making it number one in our catalog of pressing issues.

2 Data Breaches

Even though the number of publicly reported data breaches declined 8% during the third quarter from the previous quarter, these intrusions remain a perennial problem, according to the Identity Theft Resource Center.

Financial-services providers are the perennial leading target for criminals looking to steal personal data, with 141 breaches reported during the third quarter, according to the IRTC. While 2024 is unlikely to see a record number of breaches, the finally tally for 2024 will be close to 2023's record number.

So what's fueling these breaches? One factor is the emergence of new technologies that make it possible for anyone without any real technical skills or coding expertise to hack into a data base. "If you can operate a mobile phone, you can operate these tools," says James Lee, chief operating officer for the IRTC. "Just about anybody can be a data thief now."

Artificial intelligence is another new tool criminals are adopting. AI lets them write flawless scripts for phishing scams to obtain log-in credentials. These log-ins allow them to gain access to a server and launch an attack against a database.

"Automation helps criminals become more efficient in their attacks, and AI is a tool that makes criminals more efficient through automation," Lee says.

3 Antitrust Pressure

A 71-page lawsuit filed late in September against Visa Inc. by the U.S. Department of Justice has once again ushered into the payments business the specter of antitrust enforcement. The case, in which Justice contends Visa controls 60% of the nation's debit card transactions, has put the national card network under the glare of a regulator's klieg light and ushered the fear of antitrust into an industry that had for years happily set aside such concerns.

The DoJ's contention is that Visa uses pricing power to induce merchants and networks to flow their debit transactions to the San Francisco-based network giant. Indeed, it wants the court to prohibit a range of pricing, fee, and incentive tactics it says the network uses to control the share of debit transactions it gets from merchants and to win fealty from debit issuers. And while the 2010 Durbin Amendment requires issuers to offer a choice of more than one debit network, Justice contends Visa defeats that requirement with volume incentives for issuers that leave the banks with little incentive to send transactions to competing networks.

At the same time, the suit argues Visa fends off potential competition from major players like PayPal and Block by offering incentives amounting to hundreds of millions of dollars to avoid developing competing debit services.

This is not the first time the DoJ has gone after Visa, In 2021, the network dropped a $5.3 billion offer to acquire Plaid, on open-banking platform, in the face of opposition from the antitrust enforcer.

4 Checkout Friction

Cart abandonment during checkout remains a big problem in e-commerce. On average, just three of every 10 online shoppers complete their purchase, according to industry studies.

The reasons cart abandonment is so high vary from non-payment-related issues, such as taxes and shipping costs that make the overall purchase price too high, to such requirements as making consumers manually fill in their payment and shipping data at checkout.

In the latter case, if the payment process isn't handled with a card-on-file or a digital wallet, the customer must manually input their data. "That can be a hassle, particularly if the transaction is being done on a mobile device," says Thad Peterson, a strategic advisor for Datos Insights.

Another payments-related reason online shoppers abandon their carts at checkout is that merchants offer too many payment options, Peterson adds. That creates the so-called NASCAR effect in which a Web site, clothing, or object has so many logos and ad images that consumers become overwhelmed and tune out the messages.

"As payment ecosystems continue to increase in complexity, cart abandonment at the point of purchase will remain a challenge for consumers and merchants," Peterson says.

5 AI control and Fraud Issues

Artificial intelligence is one of the latest buzzwords floating around the payments and every other industry, but it isn't new to payments. Long part of fraud prevention and other elements, and known by many as machine learning, AI is now quickly being adopted by the adversaries of payments integrity and security.

Criminals are using AI to create better synthetic identities to trick organizations into seeing their attacks as legitimate. Data breaches are a prime source of valid personally identifiable information that criminals can pour into AI tools to generate synthetic identities. How much of a worry is it? Seventy-four percent of those in an Abrigo survey in August said AI's use in fraud is a concern.

Yet, payments organizations can put AI to use, too, to fight fraud. Mastercard Inc. says it uses generative AI to help predict when the full card details of a compromised credit or debit card can be used to more quickly block a fraudulent transaction. It's using AI to reduce false positives, too. FIS Inc. uses AI tech from fintech Stratyfy in its SecurLock service to better identify fraudulent card transactions.

Inversely, AI can make phishing scams more effective because the phishing emails may do a better job of getting individuals to reveal sensitive data, a Datos Insights report notes. Another concern focuses on when these models are used for phishing scams to collect consumer data. On these occasions, the scams bypass traditional fraud-detection technologies. "Generative AI is used further upstream in the scam to deceive consumers," says Trace Fooshee, a Datos strategic advisor for fraud and anti-money laundering.

6 Debit Routing in E-Commerce

For years, banks got away with routing online debit card transactions, almost automatically, to Visa and Mastercard for processing. The practice may have made for efficient processing but it happened to violate a key feature of the 2010 Durbin Amendment and subsequent Federal Reserve rule, both of which required that issuers observe merchant choice of network for debit processing, There was no exception for e-commerce.

Better late than never, the Federal Reserve in 2021 issued a clarification of its routing rule that made it plain the rule applied as much to card-not debit transactions as it did to in-store ones. No excuses. The rule clarification went into effect July 1, 2023.

That may have been a much-needed—though also much delayed—clarification, but it introduced a conundrum for banks and processors that had grown accustomed to flowing transactions to the Big Two networks. Some are still wrangling with internal procedures to ensure network choice for transactions they had formerly considered beyond the scope of other networks. These other networks beg to differ, and now they—and merchants that stand to benefit from competition for their transactions—stand to benefit.

Cyber criminals are also employing so-called bust-out schemes, which occur when a cybercrook establishes a legitimate merchant account and processes a small number of legitimate payments to establish credibility, then submits numerous fraudulent transactions and vanishes after obtaining payment, the Visa report says.

7 Practical Use Cases for Real Time

Real-time payments have been available in the United States since 2017, when The Clearing House Payments Co. LLC's RTP network launched. It got a boost in 2023 when the Federal Reserve's FedNow network debuted. While commercial real-time payments use cases were easy enough to develop, the case for them in retail payments is a little more challenging.

Among the complicating factors are the ubiquity of entrenched payment methods and consumer and merchant affinity for them, as well as the sheer number of participating financial institutions. Jumping to the latter, more and more U.S. banks and credit unions are enrolling in one or both of the U.S. real-time payments networks. The U.S. Faster Payments Council, in an October report, predicted between 70% and 80% of U.S. financial institutions will be able to receive instant payments by 2028, with between 30% and 40% being able to send them.

Among the uses cases with the most potential for development and launch are earned wage access and domestic peer-to-peer transactions. But one of the most intriguing of the use cases to emerge so far is digital-wallet drawdowns, which enable funds to be moved from a digital wallet to a bank account in real time. The appeal of these drawdowns for consumers is that they can move money out of a stored digital wallet and into a bank account immediately.

The request for payment, a relatively new service, may be a driver, too. It enables a party to send a bill digitally to another party to trigger an immediate digital payment in return. Both FedNow and RTP have request for payment capabilities. Other practical use cases, such as for e-commerce purchases and point-of-sale transactions, will require more than four years to be made available, the FPC report says.

8 Embedded Payments' Impact on Acquiring

A quick search for "embedded payments" on DigitalTransctions.net finds a few results from before 2020, with the number of posts on the subject ballooning in 2022, testament to the growing importance of integrating payments into software applications and Web sites. What's boosting the popularity of this payment option? For merchants, embedded payments provide consumers the ability to pay without being redirected to a third-party site at checkout. But the impact on processors is a little more ambiguous.

The important thing about embedded payments—a term for payment solutions natively built into an app developer's or fintech's software—is that they are said to give merchants more control over payments flows. That's because merchants can embed payment capabilities across a variety of digital touchpoints beyond the merchant's app. Such touchpoints can include micro-stores on a social-media site, a marketplace, or within an email.

"By having embedded payments, the merchant has probably eliminated a penny or two or three on [the cost of] a transaction," says Jeff Fortney, senior associate at TSG, a payments advisory firm. "It's about what you're selling to merchants today. You're selling processing. [You're] not technically selling embedded payments. [You] are selling the need to have a secure solution, a need to have something that will get you data quicker and help you sell faster."

The data is a key component of embedded payments' rise, says Don Apgar, director of merchant payments at Javelin Strategy & Research. "When we see embedded payments, there is power in the sharing of data," Apgar says. "When you start talking about embedded payments, you're talking about data sharing."

9 Merchant Saturation

The prime, so-called greenfield, days of terminalization and large numbers of merchants ripe for accepting payment cards may have passed, but opportunities for savvy payments companies have not. "There's not much greenfield opportunity left, quite frankly," says Don Apgar, director of merchant payments at Javelin Strategy & Research.

Interchange programs for supermarkets and other large retailers, coupled with the advent of the debit card—which put card-based electronic payments into more wallets than did credit-constrained credit cards—were two big pushes toward convincing merchants to adopt card acceptance. Then the debut of Square and its payment-facilitator model—called aggregation when Square launched in 2009—was another push. Square "enabled the whole bottom half of the market," Apgar says.

Today, property-management (rental payments) and business-to-business payments are attractive because cards have a small presence in them. But Apgar cautions there's a reason for that. They are complex markets with unique needs that some acquirers may lack the expertise and financial means to effectively sell to. Jeff Fortney, a senior associate at payments-advisory firm TSG, doesn't view this is as a saturation issue, but rather as one with changing merchant needs.

"The big challenge is, I can get this point-of-sale at Clover and it does all I need it to do," he says. Clover is Fiserv Inc.'s POS system. "If you stop and look at these processors, they're all looking for something to sell today," Fortney says. "So, they're getting creative."

10 Beneficial Ownership Reporting Rule

Compliance with the Beneficial Ownership Reporting Rule (BORR) has perplexed acquirers and processors ever since it went into effect in January.

Developed by the Financial Crimes Enforcement Network, BORR requires businesses, regardless of industry, to report information about individuals who directly or indirectly own or control a company. The law, however, exempts some companies from reporting, a loophole that has helped fuel confusion about the rule.

The law was developed to help combat money laundering and to prevent criminals and corrupt officials from hiding their identities.

While acquirers and processors are well aware of the law, confusion about its application persists. "It is a complex law requiring interpretations of the rules and the [exceptions] of which companies are exempt from reporting", says Scott Talbott, executive vice president for the Electronic Transactions Association.

The issue for acquirers and processors, then, is not a matter of lack of awareness, but rather one of "confusion by some individual companies about how to apply the law to their merchant base," Talbott adds.

To improve compliance. the ETA has launched an education campaign about the law's reporting requirements and implementation issues. The ETA also invited FinCEN to address members about the law at an annual conference in October. DT

USPS STATEMENT OF OWNERSHIP, MANAGEMENT AND CIRCULATION

1. Publication Title: **Digital Transactions**
2. Publication Number: **024-247**
3. Filing Date: **October 10, 2024**
4. Issue Frequency: **Monthly**
5. No. of Issues Published Annually: **12**
6. Annual Subscription Price: **$59.00**
7. Complete Mailing Address of Known Office of Publication (Not printer):
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137
   Contact Person: John Stewart Telephone: (877) 658-0418
8. Complete Mailing Address of Headquarters of General Business Office of Publisher (Not printer):
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor:
   Robert A. Jenisch
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137

   John Stewart
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137

   John Stewart
   Boland Hill Media LLC
   800 Roosevelt Road Building B Suite 212
   Glen Ellyn, IL 60137
10. Owner (If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.):
   Boland Hill Media, LLC **Same as block 7**
   Robert Jenisch **Same as block 7**
   John Stewart **Same as block 7**
11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities (if there are none, so state): **None**
12. Tax Status (For completion by nonprofit organizations authorized to mail at special rates): **Not applicable**
13. Publication Title: **Digital Transactions**
14. Issue Date for Circulation Data Below: **September 2024**
15. Extent and Nature of Circulation:

	Average number of copies of each issue during preceding 12 months	Number of copies of single issue published nearest to filing date
a. Total Number of Copies (Net press run)	22,224	22,728
b. Legitimate Paid and/or Requested Distribution (By Mail and Outside the Mail)		
1. Outside County Paid/Requested Mail Subscriptions Stated on Form PS Form 3541. (Include direct written request from recipient, telemarketing and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies)	10,120	10,898
2. In County Paid/Requested Mail Subscriptions stated on PS Form 3541. (Include direct written request from recipient, telemarketing and Internet requests from recipient, paid subscriptions including nominal rate subscriptions, employer requests, advertiser's proof copies, and exchange copies)	0	0
3. Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution outside USPS	0	0
4. Requested Copies Distributed by Other Mail Classes Through the USPS (e.g. First-Class Mail)	0	0
c. Total Paid and/or Requested Circulation [Sum of 15b (1), (2), (3), and (4)]	10,120	10,898
d. Nonrequested Distribution (By Mail and Outside the Mail)		
1. Outside County Nonrequested Copies Stated On PS Form 3541 (include Sample Copies, Requests Over 3 years old, Requests induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)	9,973	8,786
2. In County Nonrequested Copies Stated on PS Form 3541(include Sample Copies, Requests Over 3 years old, Requests induced by a Premium, Bulk Sales and Requests including Association Requests, Names obtained from Business Directories, Lists, and other sources)	0	0
3. Nonrequested Copies Distributed Through the USPS by Other Classes of Mail (e.g. First-Class Mail, Nonrequestor Copies Mailed in excess of 10% Limit mailed At Standard Mail or Package Services Rates)	0	0
4. Nonrequested Copies distributed Outside The Mail (Include Pickup Stands, Trade Shows, Showrooms and Other Sources)	840	2,382
e. Total Nonrequested Distribution (Sum of 15d (1), (2), and (3))	10,813	11,168
f. Total Distribution (Sum of 15c and e)	20,933	22,066
g. Copies not distributed	1,291	662
h. Total (Sum of 15f and g.)	22,224	22,728
i. Percent Paid and/or Requested Circulation (15c divided by f times 100)	46.5%	47.8%

16. Electronic Copy Circulation

a. Requested and Paid Electronic Copies	0	0
b. Total Requested and Paid Print Copies (15c) + Requested/Paid Electronic copies (16a)	10,120	10,898
c. Total Requested Copy distribution (15f) + Requested/Paid Electronic copies (16a)	20,933	22,066
d. Percent Paid and/or Requested Circulation (Both print & electronic copies) (16b divided By 16c x100)	48.3%	49.4%

X I certify that 50% of all my distributed copies (electronic and print) are legitimate requests or paid copies.

17. Publication of Statement Ownership for a Requester Publication is required and will be printed in the **November 2024** issue of this publication.
18. Signature and Title of Editor, Publisher, Business Manager or Owner:
John Stewart, Editor Date: October 15, 2024

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

IS VISA A DEBIT MONOPOLIST?

The U.S. Justice Department has sued Visa—again—this time over its debit network practices. The case is far from cut-and-dried.

BY **PETER LUCAS**

LAWSUITS ALLEGING anti-competitive practices are nothing new to Visa Inc. After all, the network, as well as MasterCard Inc., have been sued by the Department of Justice, merchants, and state attorneys general for decades over their pricing and business practices.

When the DoJ filed its lawsuit against Visa in September alleging anti-competitive practices in the debit market, the case was seen as a continuation of Justice's ongoing scrutiny of Visa's pricing and business practices.

Four years ago, the DoJ sued to block Visa's proposed $5.3-billion acquisition of open-banking platform provider Plaid Inc., alleging the acquisition would stymie future competition. Visa opted to settle that suit by agreeing to drop its bid for Plaid, despite its statements that it would vigorously defend itself.

Now, in its current suit, Justice alleges Visa enjoys dominance as a debit card network through exclusive contracts with card issuers. The suit contends these agreements divert volume to Visa's network using incentives plus punitive fees for routing volume outside the Visa network. The incentives include volume-based pricing, the suit says. Competing networks are thus denied the scale they need to compete, the DoJ charges.

The lawsuit also alleges that Visa induces potential competitors capable of developing their own debit products—companies such as Apple Inc., PayPal Holdings Inc., and Block Inc.'s Square point-of-sale technology unit—to become partners through generous monetary incentives.

"Even though the choice to make such payments reduces Visa's immediate profits, it nonetheless pays hundreds of millions of dollars to would-be competitors to blunt the risk they develop innovative new technologies that could advance the industry, but would otherwise threaten Visa's monopoly profits," argues the complaint.

The suit further alleges Visa's "conduct cuts off competition where it should occur today. Perniciously, it also prevents its current and potential rivals from gaining the scale, share, and data necessary to erode Visa's existing dominance."

The "dominance" the DoJ refers to here reflects the fact that more than 60% of all debit transactions in the United States run over Visa's network, "allowing it to charge over $7 billion in fees each year for processing those transactions."

The complaint alleges Visa earns more in revenue from its U.S. debit business than it does from its credit business, as of 2022. "Visa debit is core to its North American business, where Visa enjoys operating margins of 83%. But even these numbers understate Visa's monopoly power over debit transactions," the DoJ says.

As expected, Visa says it will mount a vigorous defense.

"Anyone who has bought something online or checked out at a store knows there is an ever-expanding universe of companies offering new ways to pay for goods and services," Visa general counsel Julie Rottenberg said in a statement. "[The] lawsuit ignores the reality that Visa is just one of many competitors in a debit space that is growing, with entrants who are thriving."

Rottenberg added that businesses and consumers choose Visa because it is a "secure and reliable network" that provides "world-class fraud protection" and "value."

"This lawsuit is meritless, and we will defend ourselves vigorously," she said.

CHALLENGES

Antitrust lawsuits garner big headlines, but they are by no means a slam dunk for plaintiffs or defendants. The reason, legal experts say, is that such cases are complex and feature a lot of expert testimony on complicated concepts that can be difficult for a jury to follow.

"All antitrust cases involve difficult interpretations of the law, intense gathering and analysis of economic data, and a high-level battle of experts," says Barak Richman, a professor at George Washington University Law School. The government's suit against Visa, he acknowledges, is "a complicated case."

Keeping in mind how difficult it can be for either side to prevail, here are some of the issues both sides will face, as well as the challenges Visa may face in the wake of the lawsuit.

One of the biggest challenges facing the Justice Department is proving that Visa built an illegal monopoly that has created a "moat" around its debit business. This obstacle keeps potential competitors at bay and protects Visa's market share, according to the DoJ's theory of the case.

The key question the government must answer is whether this "moat" is big enough to keep all competitors out, says Lloyd Constantine, founder, partner, and chairman emeritus at the law firm Constantine Cannon, which specializes in antitrust law.

While Constantine argues Visa has created and maintained an illegal monopoly, he notes that some of the examples the DoJ uses to make its point are questionable. Constantine has a long history of trying cases against Visa and Mastercard, first as a lawyer in the New York Attorney General's office, then later in private practice on behalf of merchants.

"While the DoJ's complaint about Visa operating an illegal monopoly is correct, its characterization of the marketplace is not necessarily accurate," Constantine says.

As an example, while the government's complaint cites several competitors harmed by Visa's practices—such as Discover Financial Services, which owns the Pulse debit network—Constantine contends many of them have the resources to compete directly with Visa if they choose.

"If you look at what the complaint says is needed to compete in the debit market, Discover has all [the ingredients], but they haven't chosen to do so. It's the same with Apple, and Apple is a far more powerful company than Visa," Constantine says.

BUILDING A MOAT

So the pressure is on the Justice Department to prove Visa's practices keep out rivals that can erode its market share, legal experts say.

"Part of making a case for a monopoly is giving the court a description of the market [and its competitive dynamics], then proving that the controlling practices keep out all competitors and maintain Visa's power over the market," says James Septa, a professor of law at Northwestern University. "Visa can argue that it has good reason for its actions and that they do not harm competition."

Another potential stumbling block for the DoJ is its allegation that Visa's contractual practices are intended to lock out competition through monetary incentives.

"It's common for payments networks to vie for volume via incentives and volume-based pricing, and you see similar examples in other industries," says Leanne Lange, managing director, client strategy, in


Grover

Grover: "It can be argued that any network with scale has built a moat around its businesses."

the payments advisory practice for SRM (Strategic Resources Management Inc.).

Part of what makes Visa stand out to the DoJ on the question of pricing incentives is that the company has been more aggressive than other debit networks, argues Eric Grover, principal at the payments advisory Intrepid Ventures. "Are some of Visa pricing strategies aggressive? Yes, but I'm not sure they are unfair," he says.

While the Justice Department claims Visa has monopolized the debit market with a more than 60% share of debit volume running through its network, that claim could be challenged by Visa.

"The market share for Visa as cited by the DoJ is substantial, but it's not an overwhelming allegation," says Septa.

He adds that many companies are hit with antitrust suits when their market share reaches 70% or higher, but the threshold for what constitutes a monopoly varies by industry.

What's interesting about Visa's debit market share is that it is lower than the 70% share the DoJ cited in its complaint contesting Visa's proposed acquisition of Plaid in 2020, says Grover.

"The market-share figures the DoJ is presenting in its current complaint suggest Visa is losing share," Grover says. "I think there is room for Visa to increase its market share, but I don't see them getting to more than the 70% or 80% level. Visa may be the biggest debit network, but debit competition is ferocious."

The PIN debit networks can't or won't compete for volume with Visa because they have positioned themselves to be more like utilities than innovators, Grover adds.

"The PIN debit networks have neutered their brands by competing on price, not by being innovative, and in some cases by being part of a large processors' portfolio," Grover adds. "It can be argued that any network with scale has built a moat around its businesses."

'YOUR WORLD CHANGES'

But Visa, too, will have obstacles to overcome. One challenge lies in proving that the exclusive contracts and deals it has entered into with debit issuers and other players are not anti-competitive.

While there is no law prohibiting exclusive contracts, courts have ruled such agreements can be anticompetitive because they can hinder a competitor that doesn't offer exclusive deals but is looking to grow its business, Septa says.

Other challenges facing Visa include lack of data to support its defense that it has not stymied competition; an unexpected piece of damaging evidence surfacing during the discovery period; and a judge who interprets antitrust law differently from Visa, says George Washington's Richman.

Outside the courtroom, Visa is likely to face challenges from debit issuers and its partners over the structure of its contracts. The partners will be looking to negotiate more favorable terms, says SRM's Lange. "The [DoJ's] lawsuit could give issuers [and partners] more leverage to open the hood on their contracts and see if they can renegotiate, Lange says.

Visa itself may even become more lenient in the enforcement of contractual penalties to avoid actions that could strengthen the DoJ's case. "When the government sues you, your world changes, because the DoJ becomes a magnet for every new complaint that falls in the realm of this case," says Constantine. "I think Visa will become more defensive about what they do and how they do it."

The big question hanging over the case is whether it will get settled out of court. Legal experts say it could be three to five years before the case goes to trial.

"If the case settles out of court, the DoJ is going want enough of a scalp to claim it won, while Visa does not want to see its debit business dismantled or core businesses practices changed," says Grover. "One of the risks of going to trial is that something catastrophic can happen." DT

Time for an attitude adjustment.

endpoint

WHY PAY BY BANK IS SAFER THAN YOU THINK

Here's why this efficient payment method is steadily overcoming doubts to establish itself as a safe, efficient—and fast—alternative to cards.

BY **DAVE GLASER**

Dave Glaser is chief executive of Dwolla

FROM INSTANT-PAYMENT processing times to real-time account access and the option to choose from multiple payment options, the modern digital economy is driven by demands to provide businesses and consumers with efficient, fast, and secure ways to conduct financial transactions.

Now, as the payments landscape evolves, financial institutions and businesses must monitor trends and spending habits while leaving room for technological advances.

One payment solution that is gaining traction in this space is pay by bank. Also known as account-to-account (A2A) payments, this method allows users to make transactions directly from their bank accounts, bypassing traditional card networks and offering a range of benefits.

Pay-by-bank transactions typically use payment rails such as the automated clearing house network, FedNow Service, and RTP network to transfer money from one bank account to another.

Despite its advantages and growing popularity in Europe and Asia, A2A adoption in the United States has been slow. This hesitancy is largely due to consumer concerns about security and privacy. However, as we delve deeper into the realities of pay-by-bank transactions, it becomes clear that these concerns are often based on misconceptions and are limiting the potential to expand the U.S. payments landscape.

UNDERSTANDING THE MISTRUST

The primary driver of mistrust in A2A transfers is fear of fraud through unauthorized transactions and potential account takeovers. In a recent report by Visa, 73% of consumers cited security and trust as the number one influence when selecting a payment type.

While security concerns with bank-to-bank transfers are understandable, they're often misplaced. In fact, compared to paper checks and credit cards, A2A transactions have the lowest fraud rates.

Indeed, when implemented with robust security measures, pay by bank can be one of the safest and most streamlined payment methods available. Customers have greater control over their payments, directly authorizing transactions and details.

Due to these added benefits, the adoption of pay-by-bank payments is on the rise. Visa's report found that 93% of U.S. consumers have made an A2A payment, and almost 70% have made a payment enabled by open banking.

As pay by bank increases in popularity, some might wonder how it differs from debit card

SPONSORED CONTENT

HOW PAYMENT TECHNOLOGY COMPANIES AND AGENTS CAN USE LOYALTY PROGRAMS

In today's cutthroat business environment, it is imperative that we as payment technology professionals find ways to help small and mid-sized businesses keep pace with their larger competitors. One highly effective way to do so is by offering a robust customer loyalty program.

According to Queue it, 65% of a company's revenue comes from the repeat business of existing customers. Meanwhile, it's at least 5x (and as much as 25x) more expensive for a merchant to acquire a new customer than it is to keep an existing one. Add in the fact that 84% of consumers are more likely to stick with a brand that offers a loyalty program while the average annual spend of members who redeem rewards is 3.1x that of members who don't, and the power of customer loyalty is clear.

Loyalty programs don't just help businesses unleash the earning power of repeat purchasers and higher customer spends, they also allow merchants to:

- Attract new customers through the positive word of mouth of their most loyal customers/brand ambassadors.
- Collect invaluable insights into their customers' preferences and purchasing patterns.
- Use that data to create more effective marketing campaigns.

Loyalty programs also pay for themselves. To wit: 90% of loyalty program owners reported a positive return on investment with the average ROI being 4.8x. Additionally, a 5% increase in customer retention can help businesses see a 25% increase in profits.

Given these figures, payment technology companies and their Agents would do well to focus on offering merchants flexible and powerful customer loyalty programs that clearly demonstrate our added value while simultaneously creating more stickiness with merchants.

Given that more than 90% of businesses now offer some form of loyalty program, it's important that the program we offer to merchants provides maximum customization and ease of use to give ourselves a competitive advantage.

By allowing merchants to tailor the program to their specific business — from how many points are required to earn a reward, to what that reward is — merchants can easily build and manage a loyalty program that keeps their customers coming through their doors while attracting new ones.

Furthermore, given that 79% of shoppers say they are more likely to join a rewards program that doesn't require them to carry a physical card, offering a digital rewards program is critically important. Modern programs that allow customers to easily track their rewards points through SMS messages and email notifications or on receipts can be very effective.

As popular as loyalty programs are already, the future for loyalty is even brighter. In fact, while the customer loyalty management market is currently valued at more than $5.5 billion, it is expected to surpass $24 billion by the end of 2028.

Are you ready to help small to mid-sized businesses drive both revenue and return visits? All while retaining and attracting more merchants than ever before? Go North to partner with the payments technology and loyalty program leader. Call 888.229.5229 or visit GoNorth.com for more details.

North

As a leading payment technology innovator, North has a diversified product platform that provides a modern end-to-end infrastructure to enable globally preferred payment types. Serving hundreds of thousands of businesses and with over $100 billion per year in electronic transaction volume, North delivers functional, feature-rich and frictionless solutions for the evolving merchant economy.

payments. The answer lies in the cost-effectiveness and efficiency of pay-by-bank transactions. For merchants, pay-by-bank transactions avoid the traditional card networks and their associated fees, making these payments generally less expensive to process than debit card payments.

Additionally, A2A transactions offer enhanced security features that aren't always available with debit cards. These include real-time fraud detection, advanced encryption, and tokenization of sensitive information. The direct bank-to-bank nature of these transactions also reduces the number of intermediaries involved, minimizing potential points of vulnerability.

SECURITY CONCERNS

To ensure the utmost security in pay-by-bank transactions, fintechs are implementing highly advanced technologies and protocols. These include:

1. Open-banking integrations that provide secure, standardized ways for third-party providers to access financial data with user consent.
2. Strong customer-authentication measures, often involving multi-factor authentication.
3. Advanced encryption and tokenization to protect consumer data and financial information.
4. Real-time transaction-monitoring and fraud-detection systems powered by artificial intelligence (AI) and machine learning (ML).
5. Robust consumer-protection policies and regulations that safeguard users against unauthorized transactions.

It's important to note that these security measures are not static. Financial institutions across the industry continue to find new ways to improve security protocols and provide innovative safety features. As potential threats emerge, so do new defensive technologies and strategies, which is where AI and ML can drastically help organizations minimize risks and address concerns as they happen.

Furthermore, the regulatory landscape is evolving to keep pace with these technological advances. Bodies such as the Consumer Financial Protection Bureau (CFPB) are working on comprehensive frameworks for open banking and A2A payments, ensuring that consumer protection remains at the forefront.

RECOGNIZING THE ADVANTAGES

The benefits of pay by bank extend beyond security. For businesses—especially those in industries with high transaction volumes or recurring payments—pay by bank offers lower fees, faster settlements, and reduced chargebacks. Consumers benefit from the convenience of digital payments and increased control over their financial data.

Pay by bank also offers significant advantages in terms of financial management and cash flow. For businesses, faster settlement times mean improved liquidity and more accurate real-time financial reporting. This can be particularly beneficial for small and medium-size enterprises that often struggle with cash-flow issues.

For consumers, pay-by-bank transactions provide a clearer picture of their spending, as the money is directly debited from their account, helping with budgeting and financial planning. Additionally, the reduced risk of overdraft fees—which are common with traditional debit card transactions—adds another layer of financial security for users.

As the U.S. market continues to adopt pay-by-bank solutions, it's crucial for businesses and consumers alike to understand both the convenience and the security aspects of bank-to-bank transactions.

The future of payments is digital, and pay by bank is poised to play a significant role in this transformation. The misplaced mistrust surrounding this payment method will likely fade as more businesses and consumers experience its benefits firsthand.

Indeed, with continued investment in security measures and user education, pay by bank has the potential to become the preferred payment method for millions of Americans, offering an impactful blend of convenience, cost-effectiveness, and security. DT