BAI Banking Strategies
Executive Report

February 2023

Banks are getting more personal with payments

BAI POWERING SMART DECISIONS.

CONTENTS

2023: The year of payments innovation

BY TERRY BADGER, CFA
tbadger@bai.org

For both businesses and individuals, faster and more secure ways to make and receive payments are a top priority, and as banking goes ever more digital, institutions have a lot riding on building up speed and safety in transactions.

According to recent research, almost two of every three owners of a small or mid-size business have cash flow worries arising from the challenges of collecting payments from their customers, which leads to difficulties staying current with their own bills. For individuals, the desire for real-time payments is in tension with the rising threat of fraud, leaving banks working toward finding the right equilibrium.

In this month's BAI Executive Report, we explore what's new in the payments space and where the sector is heading.

Our lead article by contributing writer Katie Kuehner-Hebert projects that 2023 could be a pivotal year for payments, as new products and technologies under development start being deployed for customers with an emphasis placed on personalization.

One innovative newcomer to the U.S. payments marketplace to watch is an online shopping site out of Shanghai called Temu, which enables "team purchases" that allow family members, friends and influencers to recruit other shoppers with an eye toward getting quantity discounts on their combined purchases.

Other predictions include that cross-border instant payments will also grow in prominence and scale as more businesses operate globally, and that cloud-native solutions developed for payments could open up other parts of the banking environment in a cost-effective fashion.

Enhanced identity and account takeover protections, and a deeper understanding of the "last mile" of transactions are also seen as progress areas for 2023.

On the real-time payments front, the Federal Reserve's FedNow program, expected to debut this year, which promises to greatly expand customer access to RTP and overcome obstacles and reduce operational risks for banks. Contributing writer Lauri Giesen speaks to a number of industry watchers about FedNow and whether the RTP reality will measure up to the hype. Her reporting suggests that it just might.

For customers, anticipated benefits include lower-cost borrowing and more protection from late fees. For banks, RTP redundancy and reduced payment and settlement risk are among the potential upsides. "The Fed has long had a gap in the marketspace for instant 24/7 movement of funds," one expert tells Giesen.

The most common form of real-time payments is peer-to-peer (P2P) payments via services such as PayPal, Venmo and Zelle. In the United States and elsewhere, P2P payment growth in recent years has been staggering, both in volume and in value—the global P2P market is estimated at $2 trillion-plus now, and is expected to exceed $5 trillion by 2028.

And when your dollar value begins with a T, that's going to attract more attention from criminal elements seeking to peel off some of that value for themselves.

The once-clear line between authorized and unauthorized transactions is blurring, which may put institutions on the hook for payment scams affecting customers if the customer is tricked via social engineering or other means into approving a payment or transfer, or revealing their account credentials.

For this month's Q&A, I speak with Jake Emry, a fraud prevention specialist at NICE Actimize, about the reinterpretation of the Fed's Regulation E, particularly for P2P payments, and what that could mean for banks and credit unions.

Emry explains that the Consumer Financial Protection Bureau is taking the view that, because so much of banking is now digital and fraudster schemes have gotten so sophisticated, someone who is scammed into making a payment or sharing credentials has not really authorized that transaction.

And finally, Christina Luttrell from GBG Americas (IDology and Acuant) offers her perspectives on how modern identity verification technology can help strike that delicate balance between providing the low-friction payments environment that customers crave, and at the same time, keeping them safe from the growing number of fraudsters out there prowling banking's digital streets.

She makes a case for using data-driven intelligent ID technology with a layered approach as a way to validate customers earlier in the transaction process. Doing so can help counter the dramatic upswing in synthetic identities that the industry is seeing. An added benefit of intelligent ID tech, Luttrell writes, is the ability to better locate and serve thin-file consumers, including millennials and Gen Zers, who are looking for speedier payment options.

We hope you find this Executive Report helpful as you work to enhance your payments infrastructure and offerings. Feel free to email me to let me know what you think.

Terry Badger, CFA, is the managing editor at BAI.

Payments innovation will gather steam in 2023

Industry watchers expect banks and fintech solution providers to focus on a host of products, along with a push for more personalization.

BY KATIE KUEHNER-HEBERT

Payments modernization is a hot spot within the fintech universe, with the pace of change accelerating in recent years due to more powerful technology, robust payment standards and the pandemic.

And it's shifted the entire payments ecosystem, says Nigel Prince, senior vice president, partnerships, ventures and delivery at the $704 million-asset Axiom Bank in Maitland, Florida, adding that businesses expect financial institutions to offer more innovations, including real-time payments and requests for payment.

"The ability to anticipate demand, manage reserves and provide timely settlement of amounts owed is more important than ever in this age of increasing demand, supply chain challenges and evolving consumer sentiment," Prince says.

In 2023, more small and mid-sized businesses will want financial institutions to offer a broader suite of digital financial management workflows and integrated payment solutions that can help them overcome challenges within their accounts payable and accounts receivable processes, says Keith Riddle, CEO of BankiFi Americas. His company was a finalist in BAI's 2022 Global Innovation Awards.

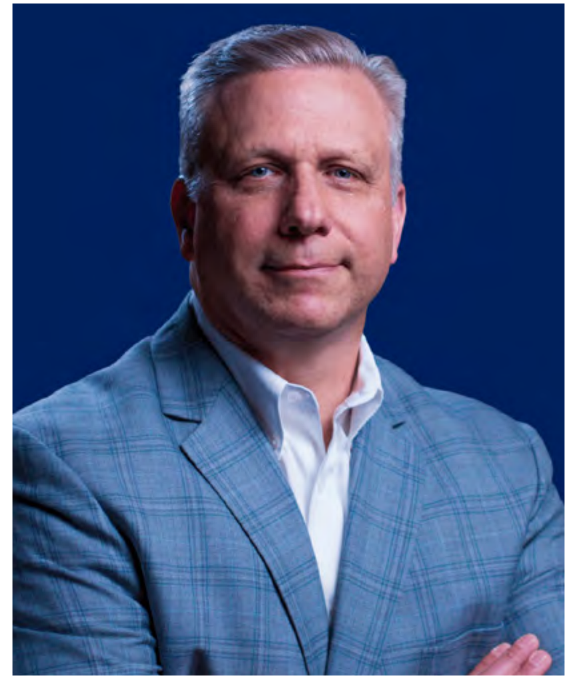
And there are challenges: 62% of SMB owners are concerned about cash-flow issues resulting from difficulties in collecting payments from customers and then paying their suppliers. A third of SMBs have more than $20,000 in outstanding invoices because they don't have a timely way to collect those payments, and nearly a third cannot pay vendors on time.

"These challenges can be solved if financial institutions offer an embedded banking platform with a set of integrated services—accounting, invoicing, payments and cash flow forecasting—to their SMB customers via an open platform, facilitating accounts receivable and accounts payable transactions, as well as impactful financial insights," says Riddle, who is based in Columbus, Ohio.

'TEAM PURCHASES' COULD SHAKE UP PAYMENTS

In the view of Richard Crone, CEO of Crone Consulting LLC in San Carlos, California, the most important payments phenomenon to track in 2023 is the entrance into the U.S. market of Temu, Shanghai-based Pinduoduo's online shopping site. Temu facilitates "team purchases" that allow micro-influencers, family members and friends to recruit others to earn quantity discounts on their combined purchases.

NIGEL PRINCE
AXIOM BANK



KEITH RIDDLE
BANKIFI AMERICAS

"Temu's unique invention is leveraging word of mouth, social sharing and 'check-in' before extending an offer versus just acknowledging a purchase afterwards on one's social feed such as Venmo, Facebook, Instagram, Twitter or TikTok, or buyer reviews on Amazon and the like," says Crone, adding that financial institutions whose retail customers use a platform like Temu can bolt on other services to expand their revenue.

"Because banks are the trusted holders of customer financial accounts, the big opportunity is to strategically offer customers and trusted partners access to those accounts, enabling payments, lending, 'buy now, pay later,' and other services in a seamless API so those functions are available to customers wherever they may be transacting," Crone says.

Other payments innovations that Crone is watching in 2023 include the modernization of "pay by bank" by retailers; acceptance of peer-to-peer payments by merchants at point of sale; and the launch of more all-in-one accounts that combine debit, prepaid, credit, BNPL and savings in a single mobile user interface.

RICHARD CRONE
CRONE CONSULTING LLC

Cross-border instant payments will also grow as businesses expand their global operations, says Burak Kutlu from Istanbul-based Payten Teknoloji A.S., a winner of a BAI innovation award for 2022. Another top priority for businesses in 2023 will be data privacy and cybersecurity to fight back against fraud that is evolving with increased digitalization.

"Thanks to growing adoption of 3D Secure 2 protocol and improvements in card tokenization, card-based payments fraud may decrease next year—however, there is an increase expected in consumer-initiated payments fraud," says Kutlu, who leads his company's operations in Turkey.

BURAK KUTLU
PAYTEN TEKNOLOJI A.S.

SIMPLIFICATION VIA API-ENABLED SOLUTIONS

Cloud-native solutions are enabling new entrants to differentiate in banking segments once thought too expensive to enter, says Sean Viergutz, banking transformation leader at PwC in Chicago. Companies that have already established API-enabled platforms are changing the game by simplifying working capital management for corporate treasurers, and reducing the cost and complexity of traditional B2B and cross-border products.

They're "demonstrating the ability to release new products that generate revenue more rapidly and

SEAN VIERGUTZ
PWC

Thanks to growing adoption of 3D Secure 2 protocol and improvements in card tokenization, card-based payments fraud may decrease next year—however, there is an increase expected in consumer-initiated payments fraud."

BURAK KUTLU, PAYTEN TEKNOLOJI A.S.

more cost-efficiently than ever before," Viergutz says. "This strategy has traditional players turning heads and keeping a watchful eye on this segment, while others are starting to ask, 'Why not us?'"

Zachary Aron, principal and U.S. payments leader at Deloitte Consulting LLP in Albuquerque, New Mexico, says the industry is at a tipping point for payments in the areas of digital identity, payments infrastructure and digital currencies.

"Right now, we are seeing capabilities being developed and embedded into digital experiences, and we expect to see trials where digital identity and security help enable a variety of payments transactions," Aron says. "We also expect to see innovation in cross-border interoperability between networks, enabling faster money movement and making it easier and more seamless for both people and businesses to make purchases when and how they want."

Digital currencies will likely evolve as U.S. regulators provide more clarity, Aron says. He and his team are also watching the decentralized finance (DeFi) landscape and how regulators and banks are engaging. They expect to see increased effort to make newer payment rails more secure, including enhanced cyber and identity protections, account takeover fraud protections, and greater assurance and understanding of the recipient at the "last mile" of the transaction.

Aron and his team also see payments players accelerating their moves to the cloud, looking for cloud-based services to support increased analytics-based services or to improve overall transaction processing.

Financial institutions will develop "truly" personalized products and services to better serve their customers, he says. These will include "just-in-time" delivery of payment, lending and insurance products that match the type of transaction that is being conducted, as well as delivering specific insights on how people or businesses use their money.

"Personalization is becoming even more important than ever," Aron says. "The No. 1 thing consumers and businesses are saying is, 'Know me.'"

Katie Kuehner-Hebert is a BAI contributing writer.

A game changer in real-time payments

The Federal Reserve's FedNow initiative promises to broaden RTP access and reduce operational risks for U.S. banks of all sizes.

BY LAURI GIESEN

The ability to make real-time payments at any time and on any day is increasingly important to both consumers and businesses. And while some companies facilitate banks' ability to offer real-time payment services to their corporate and retail customers, those options have been limited in their availability.

But when the Federal Reserve debuts its FedNow program later this year, the ability to conduct real-time payments is expected to expand exponentially.

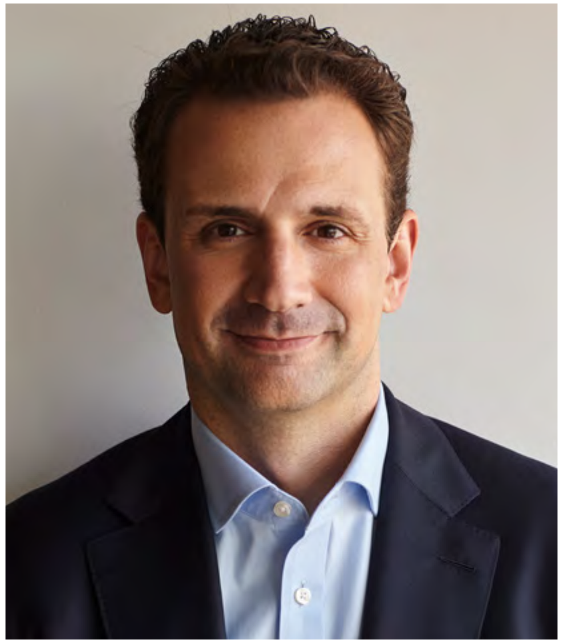
"The Fed put its full weight and confidence behind real-time payments, and that opens up a whole new world," says Chris Campbell, chief policy strategist at Kroll, a risk and financial advisory firm, and a former assistant Treasury secretary.

Making instantaneous payments in the U.S. has traditionally been cumbersome, and there have been questions about how to regulate them. "FedNow leaps over the enormous number of requirements in order to provide instant access to cash and information," says Campbell.

Others agree that the initiative will help overcome obstacles to large-scale, real-time payments initiatives in the U.S.

"There are many layers of the market that are necessary to bring payments and financial services to the lives of everyday businesses and consumers," says Carl Slabicki, co-head of global payments and treasury services for BNY Mellon. "This starts with core infrastructure providers such as the Federal Reserve or The Clearing House, and is further enabled by banks, technology services providers and corporations to leverage that infrastructure."

CHRIS CAMPBELL
KROLL



CARL SLABICKI
BNY MELLON

FEDNOW OFFERS SEVERAL BENEFITS

Consumers and businesses will benefit from FedNow in several ways. "Consumers could avoid the need to use expensive check-cashing services, engage in high-cost borrowing or incur overdraft or late fees," says Jonathan Shiery, director of financial services at Guidehouse. "Immediate access to funds and the ability to instantly make bill payments benefit small businesses that may otherwise need to seek costly short-term financing. "

Other benefits, according to Shiery, include mitigating payment and settlement risk, and strengthening resilience in the market through real-time payments redundancy.

Additionally, the service is seen as a good complement to the Fed's existing FedWire and ACH offerings. "The Fed has looked for several years for a product to sit alongside its other services," says Craig Ramsey, head of real-time and A2A payments for ACI Worldwide.

FedWire is for handling large value payments, primarily from corporations, and ACH provides a service for consumer payments, but both require overnight settlement and typically are available only during business hours. Both businesses and consumers want to move money instantly in a 24/7 fashion, Ramsey says. “The Fed has long had a gap in the marketspace for instant 24/7 movement of funds,” he says.

Some private companies offer similar services, such as Zelle from Early Warning Services and The Clearing House’s RTP, Ramsey says. But EWS and TCH are owned by some of the largest banks, which may explain why thousands of community and smaller banks have held back from offering real-time services, he says.

“FedNow will target every bank in the U.S., and as a result, we should see more real-time services offered to corporate and consumer customers,” Ramsey says.

JONATHAN SHIERY
GUIDEHOUSE

> *FedNow will target every bank in the U.S., and as a result, we should see more real-time services offered to corporate and consumer customers.”*
>
> **CRAIG RAMSEY, ACI WORLDWIDE**

And while the Fed’s involvement could compete with private initiatives to offer real-time payment services, many believe fintechs will benefit from the endeavor by developing additional channels and services to facilitate these payments.

“The launch of FedNow provides an opportunity for fintechs in the payments space to help enable financial institutions and/or their clients, both businesses and/or consumers, to gain access to such services, which can and will support a wide variety of use cases,” Slabicki says.

Use of FedNow will initially be restricted to depository institutions. But Shiery notes that the Financial Technology Association, which represents many fintech companies, is asking the Fed to make the service available without going through banks. “If we use international precedence on where FedNow will go, then we would likely see them open up access to fintechs at some point in the future,” Shiery says.

Fintechs with strong payment services should be “well positioned to continue to gain market share and customer network strength, especially fintechs in the low-dollar, peer-to-peer payments space, where funds availability is already almost immediate even if settlement on the back end happens through ACH rails,” Shiery adds.

BACK-OFFICE UPGRADES TO RUN FEDNOW

To participate in FedNow, banks will either need to make changes in their backroom operations or hire outside vendors that can do that for them. “Banks will have to make sure their back office is ready to run 24/7,” Ramsey says.

“Banks in the U.S. need to support their plans to integrate with either FedNow, RTP or both, to provide their account holders with this access,” says Slabicki. “Further, banks will need to plan for how they manage interoperability between those networks by building such themselves or working with their service providers to do so, to ensure their account holders can effectively send and receive seamlessly between both FedNow and RTP.”

In addition to the technical changes, banks will need to educate the public about the service and market it, Ramsey says. Strong risk-mitigation systems will also be needed because instantaneous payments require additional scrutiny.

“Banking institutions must familiarize themselves with the operational risks associated with changes in payments infrastructure in tandem with conducting necessary product preparation and planning,” Shiery says. “Financial institutions should continue to follow how regulators view Regulation E’s scope and protection in real-time payments as this has been an area of intense discussion.”

CRAIG RAMSEY
ACI WORLDWIDE

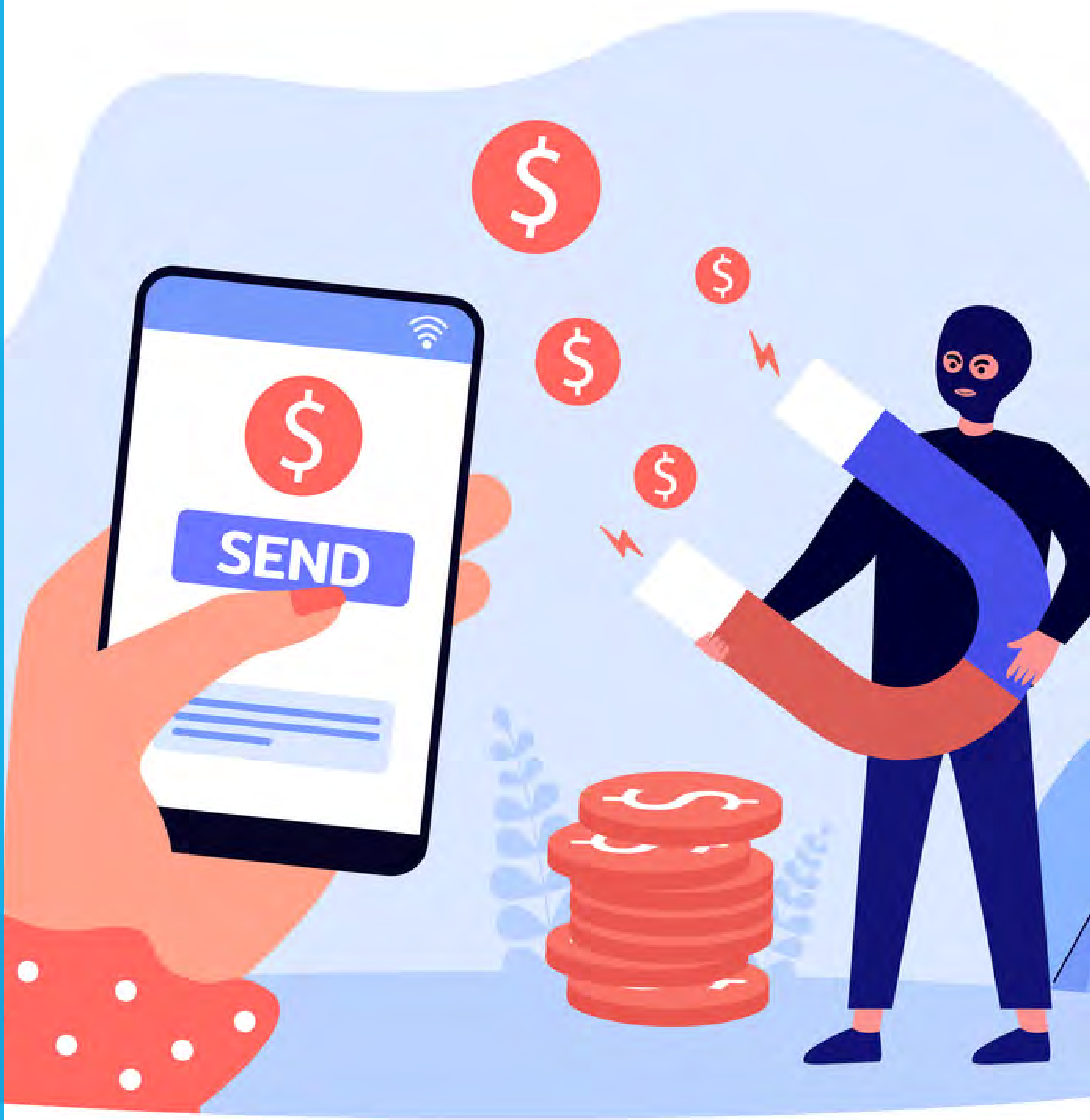
Smaller banks may not be able to provide all of this on their own, but they should be able to find service providers that can perform risk checks and deliver transactions for them, says Ramsey. Some banks may also use their existing transaction processors to provide the necessary infrastructure and services to participate.

Lauri Giesen is a BAI contributing writer.

Banks may face more liability for P2P fraud

The line between authorized and unauthorized transactions is blurring, which may put institutions on the hook for payment scams affecting customers.

BY TERRY BADGER, CFA



Fraud targeting banks and their customers is growing, and so is the potential liability for banks when it occurs.

What used to be a clear line between "authorized" and "unauthorized" banking transactions is blurring as the regulatory definition of an unauthorized transaction evolves in response to technology-driven changes in how customers do their banking and the many ways fraudsters are targeting their accounts. If a scammer tricks a consumer into giving away credentials or approving a payment or transfer, the resulting transaction could still be considered unauthorized.

Such guidance by the Consumer Financial Protection Bureau and other regulatory bodies, combined with brisk growth in social engineering scams, adds to an already challenging environment for banking institutions with regard to disputed transactions.

We recently spoke with Jake Emry, a fraud prevention expert at NICE Actimize, about how regulators are reinterpreting the Federal Reserve's Regulation E covering electronic payments, particularly peer-to-peer (P2P) payments, and what that may mean for banking institutions.

The interview has been edited for length and clarity.

BAI: Why are digital criminals increasingly targeting peer-to-peer payments?

JAKE EMRY: With social engineering, customers just seem to be very susceptible to these types of scams. If you have a mobile phone, you're experiencing it every day. Responding to these solicitations from criminals and fraudsters, clicking on these links, helps continue the facilitation of the scam. These vectors with regard to social engineering are quite concerning because even with a lot of noise in media—local and national, in print and online—about how people are being scammed by these things, it's still something that is very effective for fraudsters to use.

JAKE EMRY
NICE ACTIMIZE

What do you hear about how the federal regulatory bodies are viewing responsibilities when a bank customer is scammed?

Guidance from the CFPB is specifically focused on unauthorized transactions. They've given very specific examples of how fraudsters get into accounts through social engineering scams. For instance, the customer gives away their credentials to the fraudster. In the past, dispute teams would say, "Well, you gave the fraudster your credentials. You have some culpability there in giving a party access to your account." So they wouldn't accept liability. Well, the CFPB is saying, "No, if the customer was scammed, and you can't prove that the customer was involved in this fraud, and the customer states affirmatively,

> *There's no silver bullet for stopping social engineering-based fraud on accounts, so you rely on sophisticated means of interdiction based on artificial intelligence and machine learning and real-time payments interdiction capability."*
>
> **JAKE EMRY, NICE ACTIMIZE**

'I was scammed. Yes, I gave my credentials out,' that should be considered an unauthorized transaction of the fraud that follows from handing out those credentials." I think what the CFPB is trying to do is really clarify some of those previous loopholes—maybe some of the things that dispute teams weren't covering.

What do these interpretations and guidance mean for banks in terms of their P2P products and their fraud reduction efforts?

It's giving a hint of regulation to come. It's adding to the already challenging environment for banks with these disputed transactions. Social engineering scams are very difficult to protect against, so they require multiple layers of solution. There's no silver bullet for stopping social engineering-based fraud on accounts, so you rely on sophisticated means of interdiction based on artificial intelligence and machine learning and real-time payments interdiction capability. You can use behavioral biometrics as well to layer on top of that—knowing how the customer interacts with their account to be sure it's actually the customer logging in. I think it's going to drive a lot of solemn thought around the leveraging of those solutions, the improvements of those solutions, and evangelizing internally just how much of a problem it has been and will continue to be. These things aren't going to go away.

Greater liability in this case means greater financial risk for banking institutions, right?

This is a question that I get a lot from banks that are considering hosting their own peer-to-peer payment application, because they have a lot of concern about that liability. Their customers are going to use those third-party, peer-to-peer apps regardless, so there's only so much you can do in trying to control that activity. I would say specifically a bank should have the right risk strategy in place if it wants to open up different channels, whether it be peer-to-peer applications or crypto or whatever. It really takes a very strong risk mindset to make sure that you have the right tools in place before you enable these things for your customers because, of course, you'll have the increased liability from disputed transactions.

Why do you think this topic is not more of a public, front-burner issue for banks?

I would say it's definitely a billion-dollar issue in the industry. I think for the larger banks, there's definitely

concern about this. They're constantly enhancing their tools. Now for the smaller banks, you may not have the resources that the big multiregional banks have, and you have to really consider very carefully where you go into business channel-wise and whether you have the right controls. I think that this is definitely of concern to banks—obviously a bigger concern for some of the larger banks, where you see higher proportion and volume of peer-to-peer application activity.

Will banks have to look at more of a trade-off between greater security and delivering the instant payment execution that the customer wants?

While we're coming up to speed on faster payment mechanisms, there's an opportunity for smaller banks to be mindful about whether they have the right risk controls in place and then start to make those investments as adoption of instant payments ramps up. If your customer does experience fraud, you have four times higher risk of attrition of that customer, irrespective of how bad the fraud incident is. So these investments both have fraud prevention, but they also have retention benefits to these smaller organizations, so that they can keep those customers that they fought so hard to get and spend their limited marketing dollars and other resources on retaining them.

Terry Badger, CFA, is the managing editor at BAI.

The imperative of intelligent verification

As customers demand faster payment options, modern IDV technology can help balance fraud with friction and build a holistic view of thin-file consumers.

BY CHRISTINA LUTTRELL

The payments space is facing a multifaceted challenge. Widespread digital adoption brought on by the pandemic pushed consumers online in unprecedented numbers, leading to more convenience in online payments but also opening the floodgates to enterprising fraudsters.

And while contending with the persistent threat of fraud, the industry also needs to stay compliant with anti-money laundering and "know your customer" regulations while bringing in new customers at a rapid rate.

Intelligent and adaptive identity verification (IDV) technology is imperative to operate a compliant, growing business. And this is no easy feat: 54% of leading fintechs identified balancing fraud with friction as the greatest challenge to fraud deterrence in the industry, according to IDology's Eighth Annual Fraud Report.

Today's digital landscape requires companies to onboard and verify users in a purely digital way, and the rapid adoption of online transactions has increased opportunities for fraudsters. For example, customers of just four banks collectively experienced over $200 million in fraud using digital peer-to-peer payment service Zelle in 2021 and the first half of 2022.

Ineffective digital workflows that are either insecure or filled with friction can lead to losses in new-customer acquisition. Getting this balance right is difficult and requires organizations to leverage intelligent identity verification tech with a layered approach.

Today's digital landscape requires companies to onboard and verify users in a purely digital way, and the rapid adoption of online transactions has increased opportunities for fraudsters.

TECH TO VALIDATE CONTACT INFORMATION

Intelligent identity verification technology allows providers to validate consumers earlier in the process. Traditionally, merchants perform a credit check before identity verification. Prioritizing identity verification in this type of workflow can better position providers to confirm consumers are able to be contacted.

Ensuring that contact information is correct and that consumers can be reached is critical for providers. A provider can establish contactability by verifying information such as email, an active phone number and a fixed VOIP system while providing consumers fast access to payment tools. In the case of a "buy now, pay later" provider, if that information is not correct, then those consumers can't be reached to collect.

Payment providers need a truly intelligent solution that orchestrates enrollments or acquisitions through layers. Single-source verification often falls short of delivering the comprehensive risk perspective needed to combat the surge in synthetic identities.

By layering risk signals, such as an inactive mobile account, nonexistent email or an address risk signal, providers can better identify seemingly nonthreatening identities early in the identity proofing process and prevent fraudsters from receiving funding down the line. By screening consumers for risk within a low-friction workflow, providers can create trust with new and returning customers while keeping fraud in check.

A DATA-DIVERSE SOLUTION

Digital identity verification based on diverse data sets from a variety of authoritative sources equips providers to fight surging fraud and quickly validate consumer contact information while locating a greater variety of traditionally hard-to-find identities. With a more complete picture of a consumer's identity, payment providers can confidently locate more real customers and better serve existing customers.

Consumers, especially thin-file consumers such as millennials and Gen Zers, are looking for more and faster payment options. A growing digital landscape also means that institutions can locate and welcome individuals who may not have access to credit, utility payments or other documents that help build public records.

Millennials and Gen Zers are now two of the three largest generational groups in the U.S. but are considered harder to locate in public or credit records because they don't have lengthy banking histories. Furthermore, millennials are the largest drivers of net new-loan demand, and this trend will likely continue for most of the next decade.

The mechanisms used to locate millennials can also apply to subsequent generations, starting with the nearly 70 million Americans in Generation Z. The oldest members of Gen Z are now in their mid-20s, so they are moving into the stage of their career and family life where their need for banking services is high and growing.

An effective platform should use multiple layers of identity verification to build a holistic view of identities, especially those more difficult to locate. Fintech leaders agree that multi-layered points of verification and data verification are the best practices for successful identity verification. Identity verification powered by a diverse data set offers better anti-fraud performance while enabling transparency into which layer of fraud verification has been triggered.

STAYING AHEAD OF FRAUD

A recent study on consumer perceptions of fraud found that 68% of consumers ranked a secure digital process as the most important factor when opening a new account. Conversely, 45% of consumers said they strongly dislike companies that require additional security steps.

To be competitive in a fast-paced digital environment, organizations clearly need an advanced identity verification solution that can drive revenue and deter fraud without adding friction to the customer experience. Payment providers that fail to implement robust identity verification systems will struggle to manage evolving fraudster tactics and expose consumers to unnecessary friction.

Faced with increasing competition and a more crowded marketplace, providers must meet this challenge head-on. Intelligent identity verification technology enables businesses to confidently locate, verify and approve more legitimate customers faster—and gain a competitive edge.

Christina Luttrell is chief executive officer for GBG Americas (Acuant and IDology).

Past Issues

JANUARY 2023
Finding an edge in fraud's cat-and-mouse game »

DECEMBER 2022
Addressing banking's key business challenges in 2023 »

NOVEMBER 2022
Plotting the future of digital banking »

OCTOBER 2022
Marketing in 2023: Opportunities and challenges »

SEPTEMBER 2022
Where does digital transformation go from here? »

STAY TUNED FOR

March 2023
BANK BRANCH OUTLOOK

April 2023
MOBILE BANKING EXPERIENCE

BAI Banking Strategies
Executive Report

Banks are getting more personal with payments

February 2023

POWERING SMART DECISIONS.