BAI Banking Strategies

EXECUTIVE REPORT

Safeguarding against fraud

JANUARY 2024

BAI POWERING SMART DECISIONS.

In this issue

Bankers will be challenged in 2024 to safeguard against fraud coming from many different directions

BY EDMUND LAWLER

Fraud is hardly a banker's favorite topic, but it demands special attention this year.

As contributing writer Katie Kuehner-Hebert writes in the lead article of this Executive Report on safeguarding against fraud, swindlers are on the march on a frightening number of fronts.

Bad actors are using deep fakes, account takeovers, phishing texts and emails, application scams and check washing. They're even robbing U.S. Postal Service letter carriers to get their hands on mail that could contain a check. It's a federal crime, but the fraudsters are undeterred.

And now there's generative AI. As Rob Rendell, global head of fraud market strategy and fraud prevention for NICE Actimize, told Katie: "Generative AI, including ChatGPT, is fueling the fire for fraud. We're anticipating deep fakes, voice cloning and manipulation of photos, as generative AI will be leveraged by fraudsters to carry out their attacks. The level of sophistication will only grow as fraudsters look to leverage these sophisticated tools."

I interviewed Ash Khan, head of enterprise fraud management for BMO Financial Group. AI and now generative AI, Khan told me, allow the bank to be more efficient and effective. "The more quickly we can address potential fraudulent transactions, the better we can get at reducing our false positive rates and improving our true detection rates."

But there's generative AI's dark side, which criminals can use for nefarious purposes. "They don't need to understand complex IT systems or programming languages to create malware, to write malicious code or to create fraudulent websites," Khan says.

Contributing writer Dawn Wotapka looks at how the recent fraud rule changes by Early Warning Services LLC, owner of the popular money transfer app Zelle, will affect fraud losses and fraud claims investigations by banks. Zelle recently launched an advertising campaign to educate consumers on how to spot and avoid financial scams when a criminal pretends to be an authority figure – such as a bank representative, the government or even a business – to convince consumers to provide sensitive personal information or money.

Also in this issue:

» **Key considerations for digital identity verification in an evolving landscape:** IDology, a GBG Company's Crystal Blythe writes that unprecedented digital adoption brings new potential for revenue growth, and, unfortunately, more opportunity for fraud. One effective strategy for deterring fraud is advanced identity verification. But not all solutions offer the same level of protection. A solutions platform that provides access to a consortium fraud network backed by adaptive human intelligence and real-time velocity alerts can empower institutions to prevent fraud in 2024.

» **Providing maximum fraud protection and an optimized customer experience:** Dewald Nolte of Entersekt says that many financial services organizations seek new security solutions to keep up with continually evolving account takeover and card-not-present fraud attacks. He notes there is an alternative approach that can span multiple channels and considers the context of each digital banking and payment interaction. Context-based, or context-aware, authentication considers the originating channel, transaction context, available authentication options and customer preference to determine the most appropriate authentication option.

» **How banks should be responding to an increase in financial industry targeting:** Alkami's Jeff Chen discusses the fraud prevention efforts of banks as they strive to strike a balance between trust—providing account holders with a satisfactory user experience—and verification—protecting users and themselves from financial fraudsters. Given the ongoing global criminal interest in sophisticated financial fraud, banks will constantly be requiring new layers and levels of digital security. He addresses several key questions for banks to consider when navigating their fraud prevention efforts.

» **Why small and mid-market banks need real-time interdiction in the fight against fraud:** Eric Tran-Le of NICE Actimize writes that credit unions, community banks and regional banks must establish greater resilience and agility to survive sweeping industry transformation and proactively safeguard their customers from accelerated, ubiquitous risk. While real-time fraud detection is a significant advantage against complex fraud in the burgeoning global instant payments environment, it's useless without real-time interdiction, which is essential to identify potential threats as they occur. Mid-market institutions must implement a risk management solution that enables them to interdict suspicious transactions.

We hope this Executive Report provides you with actionable insights on a variety of measures to safeguard against fraud. In this increasingly digital era, nothing undermines trust in a financial services organization more than a fraud incident—or the risk of fraud. We invite you to share your thoughts on fraud prevention and detection.

Edmund Lawler is a contributing editor for BAI.

Fraud trends spilling into 2024

Account takeovers, phishing, deep fakes and other scams that flourished in 2023 will challenge bank security in the year ahead.

BY KATIE KUEHNER-HEBERT

When it comes to fraud, what's old is new again—sprinkled with a growing variety of fresh new scams, particularly as AI becomes more mainstream.

Fraud experts discuss how 2023 compared with prior years and what's on the horizon for this year and beyond.

"During the COVID pandemic, organized crime rings really gave banks a break, as they were very heavily focused on defrauding all the stimulus programs that were so poorly protected," says Julie Conroy, chief insights officer at Datos Insights in Boston. "But as the stimulus program dried up, 2022 and 2023 have seen a strong resurgence of all the traditional types of fraud."

Account takeover is up, as is application fraud, both significant concerns as more countries move to faster payments, Conroy says.

While the industry thought check fraud was finally under control, it came back in 2023, says Ken Allen, an industry consultant based in Nashville, Tennessee.

"The same thing happened with ACH fraud—we thought it was a little bit more under control with a lot more different technology options for moving

money around, but good old ACH fraud was also on the rise in 2023," Allen says.

Fraud trends continued to increase in 2023 as compared to prior years as technologies evolve, says Anna Kooi, national financial services leader at Wipfli LLP, who is based in Chicago.

"Automation advancements have made it easier for criminals to hack accounts and remain undetected," Kooi says. "Many times, software and/or bots are being used for tasks that previously required human intervention. This allows for increased frequency, and fraudsters can cover more ground than they could historically."

JULIE CONROY
DATOS INSIGHTS

Also on the rise: new opportunities for fraud resulting from new digital payment platforms that allow consumers and businesses to make quicker and more efficient payments, Kooi says.

In the latest NICE Actimize Fraud Insights report comparing the first half of 2022 to the first half of 2023, globally there was a 22% increase in payment fraud as societies move from cash to cashless payments. With that, there was an 18% increase in total attempted events, as well as an 18% increase in dollar volume, "which is significant," says Rob Rendell, global head of fraud market strategy and fraud prevention for the Hoboken, New Jersey–based company.

KEN ALLEN
INDUSTRY CONSULTANT

"It's not sustainable, and institutions need to take a more proactive stance curbing fraud," Rendell says.

In the U.S., there was a 33% increase in deposit fraud—fraudsters depositing checks into accounts that are later returned for fraudulent reasons, according to the report. In addition, fraudsters are securing mailbox keys by robbing letter carriers and then stealing checks out of the corresponding mailboxes.

"Fraudsters alter the checks and then deposit them into accounts under fictitious names, depleting the funds when available," he says. "The Postal Service has announced they will slowly be converting from old locks to electronic locks to curb this issue."

Check alterations are becoming increasingly more difficult to spot, especially after original checks are scanned and then destroyed, says Brandon Koeser, director and financial services industry senior analyst with RSM US LLP, who is based in Minneapolis.

Phishing attempts also saw a meaningful increase in 2023, as fraudsters took advantage of generative AI to create more "convincing and compelling" text messages and emails, Koeser says.

On real-time payment rails, it's very hard for institutions to detect unauthorized push payment fraud—fraudsters tricking people into voluntarily sending money out of their account and to the fraudsters, Conroy says. Fraudsters will then very quickly hop that money several times, so tracking it, finding it and calling it back is next to impossible.

"In the U.K., there is a liability shift that will go into effect in October of 2024 where for most forms of scam fraud, the consumer will not have liability, and there will be shared liability with the sending and receiving bank," she says. "I think a lot of countries across the globe are taking a very close look at what the U.K. is doing, with an eye to potentially emulating this."

ANNA KOOI
WIPFLI LLP

WHAT DO EXPERTS EXPECT FOR 2024 AND BEYOND?

Looking ahead, what was successful in 2023 will still be successful going forward, Koeser says.

"Fraudsters are growing increasingly more adept at adjusting processes to maximize their success and ultimately their financial gain," he says. "Check fraud, card-related fraud and phishing

attempts aren't going away; they are only growing more pronounced."

First-party fraud will also be a challenge, as this type of fraud generally increases in tougher economic times, with inflation issues and interest rates "rising the way they are, whether we're in a recession or not," Allen says.

As part of this, there will likely be a continued increase in first-party fraud via people voluntarily acting as mules for criminal networks for a share of the proceeds, he says. For example, in "shop from home" scams, fraud networks recruit and dupe individuals into purchasing goods and sending them to another location where they will get to keep one item or a percentage of the goods purchased.

"In reality, the funds being used are either the individual being scammed into buying goods for the fraudster with their own funds, or they provide them stolen payment or prepaid credentials—and thus they become a part of the fraud," Allen says.

Then, there's AI.

"Generative AI, including ChatGPT, is fueling the fire for fraud," Rendell says. "We're anticipating deep fakes, voice cloning and manipulation of photos, as generative AI will be leveraged by fraudsters to carry out their attacks. The level of sophistication will only grow as fraudsters look to leverage these sophisticated tools."

> **"Improving experience while reducing risk is top of mind for many CEOs today. The move to decrease friction is increasing the risk around cybersecurity and is putting demand on the financial institutions' talent."**
>
> **ANNA KOOI**
> WIPFLI LLP

AI-powered fraud is going to have an impact in 2024, as ChatGPT and open AI become even more mainstream, Allen says. Fraudsters can emulate voices easily, so actions like creating fake IDs and emulating a person via video or voice to fool biometrics tools are going to continue.

Meanwhile, managing cybersecurity issues can be tricky as financial institutions continue to improve their customer experience this year, Kooi says. Balancing "friction" and "fraud mitigation" becomes even more challenging as the number of systems increases.

"Improving experience while reducing risk is top of mind for many CEOs today," she says. "The move to decrease friction is increasing the risk around cybersecurity and is putting demand on the financial institutions' talent. Lack of talent is driving recent mergers of equals due to CEO retirements."

In 2024, institutions should keep a watchful eye on payment modernization, like the updates to ISO 20022 and what's happening within the U.K. financial industry with the liability shift, Rendell says. Institutions should then make sure that they have good controls in place related to scams, and that they will be able to recover lost funds should a liability shift happen here in the U.S.

"That way, they're not caught off guard and they're not having to scramble to put controls in place to appease regulators—and they'll have an understanding of what they could be on the hook for legally," he says.

Having a sound fraud posture is key as the types and forms of fraud continue to grow, Koeser says.

"Proactively educating your people and your clients to combat fraud is only one step," he says. "But also communicating effectively when you become aware of something that could lead to fraud will be key to minimizing your financial loss while maintaining customer peace of mind."

Financial institutions should also find more ways to work together to curb both existing and new types of fraud, Conroy says.

"We all need to figure out how to invest in technologies that help us get faster, more nimble and more collaborative in fighting fraud. All of these attack vectors are only going to continue to escalate," she says.

Katie Kuehner-Hebert is a contributing writer for BAI.

The twin-edged sword of AI

Banks employ the latest artificial intelligence tools to fight fraud, but so do the bad actors.

BY EDMUND LAWLER

Generative AI, the latest and most celebrated type of artificial intelligence that produces human-sounding text or images, would seem to be a godsend for fraud fighters at banks.

"Advancements in AI help us authenticate our customers," says Ash Khan, head of enterprise fraud management for Montreal-based BMO Financial Group, with nearly a trillion U.S. dollars in assets.

"If we can authenticate our customers better, we can prevent things like account takeovers," Khan says. "It helps us make decisions quickly as long as we have enough computing power, and we have access to all of the data—or what I call contextual signals."

ASH KHAN
BMO FINANCIAL GROUP

MARY ANN MILLER
PROVE

Those signals help determine if the person interacting with the bank online, over the phone or in the interactive voice response system is a BMO customer or a possible fraudster.

"AI makes us more efficient and effective, and it also improves the customer experience," Khan explains. "The quicker we can address potential fraudulent transactions, the better we can get at reducing our false positive rates and improving our true detection rates. The quicker we do that, the better the outcome for the customer."

But generative AI also has a dark side.

"From a generative AI perspective, there are potential nefarious uses of this technology," says Khan, pointing to a product sold on the dark web known as FraudGPT. Similar to ChatGPT, the aptly named evil chatbot deploys machine-learning algorithms to create malicious content like convincing phishing emails or phony landing pages.

FraudGPT has become a favorite tool of cybercriminals who are beginning to master generative AI. "They don't need to understand complex IT systems or programming languages to create malware, to write malicious code or to create fraudulent websites," Khan says.

"Previously, you could tell a scam message from a real one because it had simple mistakes like typos and grammatical errors. You don't see that anymore. Now you see messages that appear to have come from your bank."

With access to malicious AI tools, fraudsters can determine the kind of language that will resonate with a customer, whether it is a romance scam or a cryptocurrency scheme, he says.

Mary Ann Miller, who's led the fight against cybercrime and other fraud for several banks and technology firms, has seen every financial scam imaginable over the course of her 30-year career. She brings that wary perspective to her role as a member of the U.S. Federal Reserve's Scams Definition and Classification Work Group.

"Previously, you could tell a scam message from a real one because it had simple mistakes like typos and grammatical errors. You don't see that anymore. Now you see messages that appear to have come from your bank."

ASH KHAN
BMO FINANCIAL GROUP

"We are in an environment of increased fraud risk," says Miller, who is also the fraud and cybercrime executive advisor and vice president of client experience for PROVE, a leading identity verification and authentication platform. "Fraud is beginning to negatively affect the revenues at some banks.

"I have even seen banks pause and turn off their digital onboarding processes because of the rate of fraud in their application processes," she says.

> **"The bad actors are already using generative AI for voice cloning or romance scams, or using different forms of AI to duplicate people's faces. With the maturation of AI comes all its advantages. But with that comes all the responsibilities of AI."**
>
> **MARY ANN MILLER**
> PROVE

"We are starting to see that fraud is having a material impact."

AI and generative AI can be useful tools in a bank's battle against fraud. "AI can go through an automated process and help diagnose the type of fraud. Then, the investigation gets routed to the right team in the bank. They can properly classify the type of fraud that victimized the customer."

The fraud diagnostic process is critical, Miller says. "Customers often don't know how they suffered a loss. They just know they have money missing from their account. But how did it happen?" The loss could be the result of an account takeover or some form of credit card scam, she adds.

Unfortunately, fraudsters are tapping AI and generative AI to launch attacks against banks. "I often refer to it as machine versus machine," Miller says, referring to how fraudsters have become adept at using machine-learning algorithms to drive their assaults. "The bad actors are already using generative AI for voice cloning or romance scams, or using different forms of AI to duplicate people's faces."

Adds Miller: "With the maturation of AI comes all its advantages. But with that comes all the responsibilities of AI."

Banks, which must balance security and privacy against providing a frictionless customer experience, are in a tough spot. "But if you really look for innovation, you don't have to trade off customer experience for security. You can have both," Miller says. "You just have to invest and think wisely about customer experience design and make sure you have the right process and controls in place to enable the type of experience the customer expects."

Security is a paramount concern of customers, according to a survey of 1,000 consumers in September for BAI Outlook Banking Outlook: 2024 Trends. When asked to list the top ways banks and credit unions can help them manage their money more effectively, consumers cited "provide better fraud and identity theft protection" as their number-one priority. The second leading priority was to "provide faster payments and quicker money transfers."

In a survey of 102 financial services organizations for the same BAI report, more than half (58%) said they are using AI to address fraud or plan to within the next year.

As BMO's Ash Khan says: "We are going to see lots of great uses of generative AI that will improve our lives and help us improve the customer experience. But at the same time, the fraudsters are going to be looking for opportunities to use the same technologies for nefarious reasons. We need to make sure that we fully understand the technology and that we stay abreast of changes when that happens."

Edmund Lawler is a contributing writer and editor for BAI.

Zelle taps Hollywood star to fight fraud

The digital payments powerhouse educates consumers on avoiding scams.

BY DAWN WOTAPKA

Zelle has gone Hollywood.

The brand known for helping move money almost instantly recently announced that actress and producer Christina Ricci will star in a campaign. Instead of a rom-com or a murder mystery, this one is designed to educate consumers on how to spot and avoid financial scams when a criminal pretends to be an authority figure—such as a bank representative, the government or even a business—to convince consumers to provide sensitive personal information or money.

The announcement follows an even bigger plot twist from Early Warning Services LLC, Zelle's network provider: "As of June 30, 2023, our bank and credit union participants must reimburse consumers for qualifying imposter scams," a spokesperson

said. “The change ensures consistency across our network and goes beyond legal requirements.”

The new standardized rules apply to all 2,100 participating bank brands on the Zelle Network. Bank and credit union participants must reimburse consumers for qualifying imposter scams, the spokesperson added.

The news was cheered by industry watchers. “The rule changes are a positive step toward protecting consumers and fostering trust in Zelle,” said Harman Singh, director at Cyphere Ltd., a cybersecurity services company. “Initial adjustments are expected. The long-term impact will be beneficial for both consumers and banks.”

The decision “reflects a positive step toward enhancing consumer protection,” said Mark Stewart, an accountant for Step By Step Business. “Acknowledging the financial toll of such scams, this move goes beyond legal requirements, showcasing a commitment to addressing emerging challenges in peer-to-peer payment security and safeguarding users against fraudulent activities.”

Singh sees bigger changes ahead: “The new rules are likely to drive innovation in the P2P payments space. Enhanced security measures could attract new users and increase overall market adoption,” he said. “Long-term benefits are anticipated. Enhanced consumer protection and clearer liability guidelines should ultimately reduce overall fraud losses.”

Zelle’s popularity has exploded in recent years: That’s meant increased convenience for consumers who can almost instantly pay for everything from food to fashion. But it has also meant increased fraud as scammers found creative ways to trick consumers, many who found there was little recourse.

In March 2022, The New York Times published a story titled “Fraud is Flourishing on Zelle. The Banks Say It’s Not Their Problem.” The article cited statistics from Javelin Strategy & Research, an industry consultant, stating that “nearly 18 million Americans were defrauded through scams involving digital wallets and person-to-person payment apps in 2020.”

In April 2022, two U.S. senators wrote a letter to Al Ko, then CEO of Early Warning: “Given the rise of increasingly sophisticated scams on your platform and the widely documented difficulties consumers have faced in seeking relief from banks, we seek to

HARMAN SINGH
CYPHERE LTD.

MARK STEWART
STEP BY STEP BUSINESS

understand the extent to which Zelle allows fraud to flourish and the steps your company is taking to increase consumer protection and help users recover lost funds."

U.S. Senator Elizabeth Warren of Massachusetts followed with a blistering report stating that:

» *Fraud and theft are rampant on Zelle—and are increasing;*

» *Banks are not repaying the vast majority of cases where customers were fraudulently induced into making payments on Zelle. "Overall, four banks that provided data reported over 190,000 cases of scams—cases where customers reported being fraudulently induced into making payments on Zelle—involving over $213 million of payments in 2021 and the first half of 2022. In the vast majority of these cases, the banks did not repay the customers that were defrauded"; and*

» *Banks are not repaying customers who contest "unauthorized" Zelle payments—potentially violating federal law and Consumer Financial Protection Bureau rules.*

"These changes underscore Zelle's dedication to service improvement and address the fraud issues it has grappled with. It's crucial for the industry to keep abreast of these developments and adjust their practices as needed to ensure better protection for consumers."

SCOTT DEPERALTA
SCOTT DEPERALTA CONSULTING LLC

SCOTT DEPERALTA
SCOTT DEPERALTA CONSULTING LLC

While Zelle points out that "from 2022 to 2023, we've seen more than 99.9% of Zelle transactions reported without fraud or scams," that small number of problematic transactions creates big issues for consumers.

"These modifications have been largely spurred by mounting pressure from lawmakers and numerous consumer complaints about payment scams," said Scott DePeralta, president of Scott DePeralta Consulting LLC. "These changes underscore Zelle's dedication to service improvement and address the fraud issues it has grappled with. It's crucial for the industry to keep abreast of these developments and adjust their practices as needed to ensure better protection for consumers."

According to Singh, "Banks need to transparently communicate the new rules and fraud risks to their customers. Multi-channel educational campaigns can raise awareness and promote safe Zelle usage."

Enter Christina Ricci: In November, Zelle announced the S.A.F.E. Squad - which stands for the Scam and Fraud Elimination. It's designed to educate U.S. consumers about safe payments usage and raise awareness about payments safety. Ricci stated: "As someone who has been targeted by scammers, I am thrilled for the opportunity to partner with Zelle to help educate people, raise awareness about fraudulent payment schemes and arm consumers with ways to protect themselves before they fall victim to a scam."

With the announcement, Zelle is essentially making consumers the star of their own fraud-prevention movie.

Dawn Wotapka is a contributing writer for BAI.

Preventing fraud in 2024

Key considerations for digital identity verification in an evolving landscape.

BY CRYSTAL BLYTHE

Digital adoption has expanded at a massive rate—more people are operating online than in previous years, and they plan to stay online. This unprecedented digital adoption brings new potential for revenue growth and more opportunity for fraud.

One effective strategy for deterring fraud is advanced identity verification, but not all solutions offer the same level of protection. A solutions platform that provides access to a consortium fraud network backed by adaptive human intelligence and real-time velocity alerts can empower institutions to prevent fraud in 2024.

Consumer expectations continuously challenge financial institutions. The pace of digitization has allowed institutions to reach more consumers in new ways, but these methods can also be exploited by fraudsters. As fast as the digital world accelerates, fraud stays one step ahead.

A new bank account was second behind a social media account, suggesting that a wide variety of consumers are ready to bank more. However, institutions risk losing customers if digital interactions are not seamless and secure.

In a highly digitized environment, there is huge potential for growing commerce, but this comes with a lot of risk. Forty-six percent of consumers surveyed in GBG's Global State of Digital Identity signed up for a bank account in 2023. A new bank account was second behind a social media account, suggesting that a wide variety of consumers are ready to bank more. However, institutions risk losing customers if digital interactions are not seamless and secure. With modern identity verification technology, institutions can meet these challenges head-on.

THE IMPACT OF AN EVER-EVOLVING FRAUD LANDSCAPE

With fraud on the rise, transacting with trust should be a fundamental aspect of operating in

the digital space. One in seven consumers say they have been a victim of fraud in 2023, and over half of businesses experienced known or suspected fraud attempts. Given that 37% of consumers have abandoned signing up for a new online account due to the process being untrustworthy, institutions must deter fraud while instilling trust.

A lack of trust causes consumers to be more skeptical of who they share their personal information with. For example, 220 million consumers reported being selective about which companies they do business with that require personal identity information. Consumers are also motivated to move on if it means a better experience, with 70% saying they are considering switching financial service providers. So, losing a customer's trust when the security or experience of a digital interaction fails to meet their expectations can have significant and long-lasting implications, especially if competitors can deliver a better experience.

BETTER PROTECTION WITH BETTER IDENTITY VERIFICATION TECHNOLOGY

Financial institutions can better protect themselves and consumers against fraud without adding unnecessary friction with intelligent identity verification technology. Correctly implementing automated, multi-layered identity verification can streamline orchestrated workflows and apply friction only as needed to the right consumer at the right time for more effective onboarding that also fosters loyalty and builds long-term relationships.

An orchestrated, multi-layered approach to fraud prevention not only protects institutions and their account holders, but also provides a distinct competitive advantage with the right attributes:

Consortium fraud network

- *Financial institutions can stay ahead of shifting fraud tactics and improve decisioning accuracy with real-time, cross-industry consortium intelligence.*
- *Fraudsters can jump from industry to industry as they carry out their plans, yet proprietary databases provide only a limited view of these novel attacks and behaviors. A consortium fraud network amplifies real-time fraud intelligence between companies and industries. With best-practices insights into fraud threats trending in other industries, institutions can strengthen their fraud management system while decreasing the risk of fraud and the associated management costs.*
- *Bad actors tend to take a scattergun approach to digital scams, targeting multiple businesses with fraudulent identities. By developing a data-sharing network between industries, all businesses can benefit from real-time fraud intelligence and start to build up a global view of digital identities that will become increasingly valuable in the battle against fraud.*

Real-time velocity alerts

- *Staying ahead of fraud can seem like a daunting task. Synthetic identity fraud (SIF) has been a historical challenge within the financial industry and is growing globally across all sectors. SIF ranked among the fastest-growing financial crimes worldwide and topped the chart as one of the most significant cross-industry fraud risks.*
- *Real-time notifications from a team of dedicated fraud analysts on high-risk activity can help financial institutions stay ahead of trending fraud. With accurate velocity alerts, institutions gain visibility into fraud patterns and can monitor high-velocity attempts. Institutions can then set limit-specific attributes associated with known fraud like SIF.*
- *With the right identity verification partner, institutions unlock enhanced scalability, allowing them to maximize their workflows. Velocity alerts act as undercurrents in the KYC process, running silently in the background. Institutions can then focus the scope of velocity rules and escalate based on organizational needs.*

Human-powered AI

- *AI is a growing force that can have a major impact on fraud prevention, but it also comes with clear risks. When implemented with human supervision and intelligent verification technology, it becomes invaluable. AI benefits from experts charged with oversight*

of incoming data and outputs. A trained fraud analyst accompanying AI-based solutions can catch new and established fraud trends, including novel threats that AI solutions may miss.

» *By pairing human-supervised AI with solutions like data, document and selfie verification, businesses can maintain compliance, streamline customer onboarding and prevent fraud at origination. This combination empowers businesses to take a multi-layered approach to combat fraud threats. A multi-layered approach creates sufficient hurdles for fraudsters while making it seamless for legitimate customers to prove their identities.*

A WINNING DEFENSE

A vital component of any fraud prevention strategy is ensuring a layered defense against evolving threats. Velocity alerts are instrumental in significantly lowering fraud rates, especially in the financial industry. A fraud consortium offers another layer of protection for consumers by sharing data that contains known fraudulent activity. With an approach to AI and ML that includes expert human oversight, institutions can ensure transparency and automation in their fraud prevention strategy.

Institutions can gain greater protection against trending threats like SIF when they combine these tools. Partnering with the right provider can empower institutions to customize and scale rules to fit their business needs.

With the right combination of fraud management solutions, FIs can keep more fraud out of their organization while creating safer digital experiences for customers.

Crystal Blythe is vice president of customer success and fraud prevention at IDology, a GBG Company.

Context-based authentication

Providing maximum fraud protection and an optimized customer experience.

BY DEWALD NOLTE

To keep up with continually evolving account takeover (ATO) and card-not-present (CNP) fraud attacks, many financial institutions (FIs) seek new security solutions to patch over each new threat. Fortunately, there is an alternative approach for FIs that can span across multiple channels and considers the context of each digital banking and payment interaction.

Context-based, or context-aware, authentication considers the originating channel, transaction context, available authentication options and customer preference to determine the most appropriate authentication option.

Every day, FIs and their customers are bombarded by threats to their hard-earned assets. To protect their customers, FIs need the ability to determine friend from foe in real time, while still offering a customer experience that supports, rather than disrupts, their banking and payment journeys. Shifting to a more holistic authentication approach may be the answer.

Per Gartner: "Most banks have multiple fraud detection platforms, typically deployed at the banking product level (e.g., debit cards, wire transfers, digital banking channels), resulting in gaps between silos open to exploitation by fraudsters."

By unifying banking services on a central platform, banks and credit unions can cover any gaps in security, plus fast-forward their digital transformation journeys, by offering a customer experience that helps them remain competitive. For issuers in particular, this would also translate into fewer false declines, fewer chargebacks, less first-party fraud and increased transaction success rates.

MOVING BEYOND THE LEGACY BACKSTORY

While there may be departments or teams that champion modern security and fraud prevention solutions, the reality is that the old ways are often entrenched by technological limitations. Another remnant from this era is the belief that fraud prevention and security are two separate challenges, with separate budgets and defense mechanisms. Unfortunately, this fragmented approach can prevent cross-communication and data sharing between these systems.

However, FIs have not been sitting on their hands as fraudsters dream up new attacks. In many cases, their defense strategy started with building a platform to support one-time password (OTP) technology. Then, as digital banking fraud evolved, fraud prevention technology evolved too. And as FIs came across the need and budget, they added security measures to their banking platform—but not necessarily from the same vendors or with the same functionality. Yet, by blocking security gaps one by one as they pop up, the systems tasked with security and fraud prevention don't necessarily work together or share intelligence, nor can they offer sufficient resistance to today's advanced fraud schemes.

"94% of FIs have recently or are planning to make changes to their authentication method. FIs are realizing the heightened susceptibility of OTP interception via text and email," reports Datos Insights, 2023.

What's more, fraudsters now leverage powerful technologies like AI to create compound attacks that can easily penetrate a bank's legacy platform. They deploy multiple attack vectors in a single attack, rendering "legacy spaghetti" ostensibly useless as a defense.

CURRENT TRENDS IN UNIFYING DIGITAL BANKING SERVICES

An industry shift is underway to unify digital banking services, so banks remain competitive and customer-centric. This concept of unification encompasses the entire user experience. It's about recognizing the customer and delivering contextual information or services based on what may already be known about them as a valued customer in other channels, and giving them a significantly more consistent, streamlined and personalized experience—one they'll remember for the right reasons.

"By 2025, 50% of new fraud detection solutions for banking will be customer-centric platforms deployed across products and channels, replacing multiple siloed solutions, for better customer experience and fraud detection," as Gartner stated in 2022.

By unifying banking services on a strategic central platform, FIs can scale quickly to adopt new solutions that shield against today's fraud schemes while proactively adapting to future needs. The bottom line—they'll have the tools to continually improve the customer experience and remain competitive, even with emerging neobanks and other challengers at their heels.

"By 2025, 50% of new fraud detection solutions for banking will be customer-centric platforms deployed across products and channels, replacing multiple siloed solutions, for better customer experience and fraud detection."

GARTNER

CLOSE SECURITY GAPS WITH CROSS-CHANNEL AUTHENTICATION

According to a report by Datos Insights, CNP fraud losses are predicted to reach approximately $13 billion by 2026. And while closing security gaps can feel like an infinite cycle, cross-channel fraud prevention is the only way to safeguard FIs and their customers from these losses.

When a fraudster steals credentials, they will try every channel in real time to find the right one—the one that fails to detect them. When

A unified, or context-based, authentication strategy covers all of an FI's customer engagement channels and shares context about each transaction, like the user's device, location and behavioral biometrics between the channels.

authentication is managed in silos, with a different provider for each channel, the opportunity to share risk signals across channels that would otherwise block the fraudster's incursion is lost. For instance, when a hacker is blocked from four channels, but the fifth fails because it was not alerted to the risk detected in the other channels, they get in. In that moment, an FI has not only failed their customer, but likely also lost that customer.

By implementing a cross-channel authentication strategy, FIs can save on the cost of fraud, prevent breaks in customer trust and prevent the risk of losing top-of-wallet status.

CONTEXT-BASED AUTHENTICATION HELPS IDENTIFY REAL CUSTOMERS

Customers want to be assured that their online transactions and payments are secure. A unified, or context-based, authentication strategy covers all of an FI's customer engagement channels and shares context about each transaction, like the user's device, location and behavioral biometrics between the channels. As a result, it silently recognizes the real customers without disrupting their transactions. It also immediately spots higher-risk activity and steps up authentication measures or blocks the transaction, using the same risk signals, like biometrics or payment behavior, to quickly determine friend from foe.

With this unified approach to fraud prevention, FIs can recognize their customers across all channels—from online, mobile, call center and branch, to 3-D secure card authorization—reducing both fraud and friction.

Ultimately, a unified fraud prevention strategy brings together the right resources to effectively fight ATO and CNP fraud, reduce false declines and chargebacks and ensure customers remain their FIs' biggest fans.

Dewald Nolte is co-founder and chief strategy officer for Entersekt.

Balancing trust and verification

How banks should be responding to an increase in financial industry targeting.

BY JEFF CHEN

"Trust, but verify" is a well-known warning in business. It's a phrase that could fit just as well within the fraud prevention efforts of banks as they strive to strike a balance between trust—providing account holders with a satisfactory user experience—and verification—protecting users and themselves from financial fraudsters.

Given the ongoing global criminal interest in sophisticated financial fraud, banks will constantly be requiring new layers and levels of digital security. Following are key questions for banks to consider when navigating their fraud prevention efforts.

WHAT AREAS ARE BEING TARGETED WITH FRAUD RIGHT NOW?

The 2023 AFP Payments Fraud and Control Survey by J.P. Morgan revealed that 65% of organizations were victims of payment fraud attacks or attempts last year. Payment fraud is expected to continue increasing and is projected to cost $40.62 billion in 2027.

A top driver of fraudulent payment attacks is account takeover (ATO). Meanwhile, check fraud continues to be an issue for many institutions and is cited as the payment method most vulnerable to fraud. Additionally, instant payment solutions such as Zelle, FedNow and RTP (Real-Time Payments) are gaining attention. These payment rails are convenient for end-users, but also for fraudsters.

From a digital perspective, imposter fraud scams are skyrocketing, according to the Federal Trade Commission. They often start with a fraudster impersonating a consumer or business by using stolen identities to open a new account at a bank or by gaining credential access and posing as the user in the digital banking environment. It is imperative for financial institutions to have a layered approach to security and fraud prevention with tools like behavioral biometrics and transaction anomaly detection. It's equally as important for banks to be prepared with guidance to minimize the impact of fraud, as they are most often the first call a business or consumer makes when fraud occurs.

WHERE IS THE FINANCIAL INDUSTRY HEADED IN TERMS OF FRAUD PREVENTION?

Fundamentally, fraud prevention is a delicate balance between protection and the user experience. As fraud and data breaches become more prevalent in our everyday lives, banks should not be afraid to tilt their trust/verify stance to the security side. However, banks need to be sure that the added security does not create unnecessary friction in the user's experience, as account holders still demand 24/7 access to their funds and the ability to transfer payments instantly, while also trusting their information and accounts are safe.

Post-pandemic fraud has evolved into a large-scale business. Fraud cost American consumers $8.8 billion in 2022, according to the Federal Trade Commission, up 44% from 2021. Well-funded, widespread networks are being deployed on an ongoing basis to conduct fraud, and their organizers are willing to spend money to make money, as if they're a legitimate business. This makes the fraud attacks more patient and complex. Data breaches in seemingly unrelated industries, such as healthcare, are fuel for financial fraud, as they give these fraud networks information for engaging in pervasive social engineering attacks.

WHERE IS TECHNOLOGY INNOVATION HEADING IN TERMS OF FRAUD PREVENTION?

Artificial intelligence (AI) is going to increase the intensity and depth of attacks, such as by using deep fakes (digitally generated imagery, audio and video) to attempt to gain account access. Conversely, AI will also be deployed by vendors who serve to protect financial institutions and their end users.

Unfortunately, an increase of widespread data breaches across the tech industry, coupled with the fact that most Americans use weak passwords across multiple accounts, creates ongoing password-based security risk. Fortunately, there is increasing interest in fintechs to improve and adopt password-less and biometric identity management solutions, which the industry believes will offer greater digital security.

Criminals will be quick to experiment with nascent technologies, such as AI, deep fakes and botnets (automated mass attacks), for their attempted fraud efforts. Financial institutions need to defensively match all new offensive criminal strategies and tactics by staying knowledgeable on current fraud patterns, educating account holders and partnering with technology providers that can outmaneuver them.

Unfortunately, an increase of widespread data breaches across the tech industry, coupled with the fact that most Americans use weak passwords across multiple accounts, creates ongoing password-based security risk.

WHAT ACTIONS SHOULD FINANCIAL INSTITUTIONS TAKE TO PROTECT AGAINST FRAUD, NOT ONLY FOR THEMSELVES BUT FOR ACCOUNT HOLDERS?

It starts by taking a layered approach to fraud prevention. At a high level are layers of fraud protection based on elements such as transactions ("Does this transaction look normal?"), authenticity ("Are they behaving like a bot or a human?") and identity ("Is this person who they say they are?").

The layered approach should also include education and account activity alerts. Financial institutions should critically engage and educate account holders, who are often the best line of defense for their own money. Setting up alerts for each instance of money movement or each time someone uses banking credentials can combat fraudulent activity.

Financial institutions also need to educate and train their staff on evolving fraud threats and patterns across the spectrum of the business.

WHAT IS THE IDEAL LAYERED APPROACH TO SECURITY FOR BANKS?

Safeguard your financial institution with a system built to uncover threat intelligence and detect and mitigate phishing, pharming and malware attacks. Financial institutions must have a multi-layered security approach that defends users, financial institutions and the technology infrastructure.

A truly prepared bank will also extend protections beyond retail accounts into business banking by meeting Federal Financial Institutions Examination Council (FFIEC) compliance objectives. Through optimized treasury management solutions, banks can prevent stolen funds resulting from account takeover, unauthorized transaction changes and fraudulent checks. Transactions should be automatically flagged and businesses should be notified in seconds when anomalies are detected.

WHAT DOES A BEST-IN-CLASS MULTI-LAYERED SECURITY APPROACH INCLUDE FOR 2024?

- *ACH and check positive pay*
- *Merchant card fraud detection*
- *Behavioral biometrics*
- *Transaction anomaly detection*
- *Suspicious digital banking activity pattern detection*
- *Two-factor authentication or one-time passcodes*
- *Dark web monitoring and real-time alerts*

The first call a business or consumer makes when fraud occurs is to their financial institution. The fraud that happened yesterday to a local big box retailer is potentially coming for a financial institution tomorrow. In addition to financial losses, instances of fraud can generate negative publicity and tarnish a financial institution's reputation, which can be detrimental to its success. Banks should make sure their branch and call center staff understand new means of fraud and how to spot it to maintain a comprehensive fraud detection system. 2024 is the year that audio, video and photo evidence cease to be trustworthy on their own.

Jeff Chen is vice president of product management at Alkami.

Beyond detection

Why small and mid-market banks need real-time interdiction in the fight against fraud.

BY ERIC TRAN-LE

Mid-market and small financial institutions (FIs) face an onslaught of unprecedented challenges amid technological, regulatory and payment disruption, including the following:

- *Existing attack vectors are increasingly enhanced alongside the democratization of large language models (LLMs) that can further ease the pathway to faster payouts via sophisticated social engineering, authorized push payment (APP) scams, synthetic identity fraud and new account fraud.*
- *Evolving regulatory activity and more stringent reporting requirements are reshaping imperatives for continuous modernization across risk management and compliance programs.*
- *Surging real-time payment (RTP) volumes, spurred by the recent introduction of the FedNow service, accelerate the urgency to adapt infrastructures to accommodate real-time fraud detection and interdiction.*

Credit unions, community banks and regional banks must establish greater resilience and agility to survive sweeping industry transformation and proactively safeguard their customers from accelerated, ubiquitous risk. While real-time fraud detection is a significant advantage against complex fraud in the burgeoning global instant payments environment, it's useless without real-time interdiction.

Real-time fraud detection is essential to identify potential threats as they occur. However, without real-time interdiction, smaller banks lack a strategic defensive pillar in their fraud management framework. To effectively safeguard customers and organizations against faster payment fraud, small and mid-market FIs must implement a risk management solution that enables them to interdict suspicious transactions before they exit the institution.

WHY REAL-TIME INTERDICTION?

Globally, fraud and financial crime are anticipated to impose a financial burden of nearly $41 billion on FIs by 2027. The FedNow launch in the U.S. is also projected to contribute to a 32.6% increase in real-time payment volume within the same time frame.

The global economy is increasingly oriented toward expeditious product and service delivery, and payment ecosystems are transforming to accommodate these accelerated transactions. As RTP system adoption escalates among FIs of all sizes to strengthen competitive advantage

and sustain customer loyalty, organizations must implement advanced protection against real-time fraud. Additionally, FedNow mandates require all participating FIs to undergo a certification process establishing their readiness to combat instant payment fraud with the appropriate communications and operational tools.

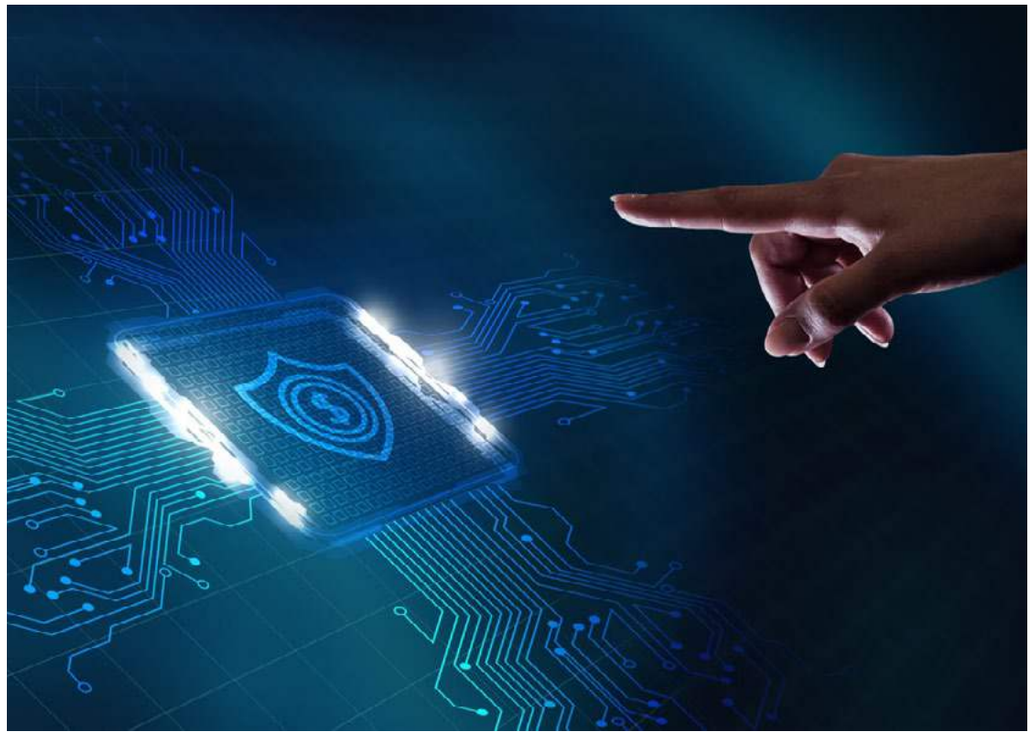
Yet, small and mid-market FIs may struggle to join the real-time payments ecosystem given the operational and resource limitations that impede infrastructure modernization efforts and intensify risk exposure. Compared to their larger peers, smaller FIs tend to lag in leveraging artificial intelligence (AI) and machine learning capabilities at just 44% in 2023 versus 66% of FIs with over $5 billion in assets.

AI- and machine learning–powered, real-time fraud prevention solutions are becoming synonymous with seamless banking experiences that can efficiently protect consumers and institutions against diverse fraud and scam typologies. However, not all real-time fraud detection capabilities are created equal.

AI- and machine learning–powered, real-time fraud prevention solutions are becoming synonymous with seamless banking experiences that can efficiently protect consumers and institutions against diverse fraud and scam typologies. However, not all real-time fraud detection capabilities are created equal.

Mitigating real-time payment fraud and associated fraud losses demands real-time fraud detection and interdiction capabilities. The ability to instantly interdict via a holistic fraud prevention solution enables small and mid-market FIs to:

- *Instantly block potentially anomalous or fraudulent transactions as they occur without disrupting legitimate transactions*
- *Dynamically adapt to new fraud tactics and enable a proactive defense against constantly evolving threats*
- *Automate responses to fraud incidents, reducing operational costs and reliance on extensive manual intervention*
- *Meet customer expectations for swift protection against complex scams and fraud, fostering customer trust and demonstrating a commitment to security leadership*
- *Prevent interruptions to customer accounts and transactions to enable a slick, convenient and real-time banking experience*
- *Bolster regulatory readiness via real-time detection and prevention of fraudulent activities, mitigating the risk of possible regulatory breaches*



THE REAL-TIME INTERDICTION DIFFERENCE

Deploying real-time fraud detection without the ability to interdict is like having a warning system that can swiftly identify suspicious activity—but the action stops at raising the alarm. When real-time interdiction is enabled, identified threats can be immediately intercepted and thwarted before losses are incurred.

In modern risk management, the true differentiator lies in interdiction. Without this capability, the chasm between identifying and preventing risk widens, leaving customers and FIs vulnerable.

Fraud can have a disproportionate financial impact on smaller banks. Unlike larger institutions, small and mid-market banks might not have the financial capacity to absorb substantial losses, making it increasingly critical to interdict in real time to minimize losses by stopping suspicious transactions before they're completed.

RTP systems like FedNow can open the door for small and mid-market FIs, granting access to opportunities that were previously beyond their reach. However, a multi-layered approach to fraud detection is crucial to facilitating a robust

Small and mid-market FIs must instantly extinguish these threats and secure their financial ecosystems with real-time fraud detection and interdiction. When safeguarding customer trust and financial integrity, it's the decisive action in real time that defines the true modernity of a bank's defenses.

response against the social engineering–based scam and fraud typologies that exploit RTP systems' immediate and irrevocable nature.

Key components of an advanced fraud detection solution that enables FIs to interdict in real time include:

- *Copious quantities of transactional and contextual data from diverse sources, including customer behavior, transaction history and device information*
- *Intelligent pattern recognition to discern between legitimate transactions and deviations that may indicate fraudulent activity*
- *Real-time monitoring to evaluate each event against learned patterns and enable instantaneous identification of anomalies as they occur*
- *Early attack stage detection that facilitates real-time intervention before any money movement happens, improving loss prevention*
- *Behavioral analytics to assess both individual transactions and broader user and entity behaviors based on factors such as transaction frequency and interaction patterns*
- *Continuous self-learning capabilities that automatically adapt in real time to new attacks and evolving customer behaviors, enabling the system to remain effective over time*

Like moths to a flame, fraudsters are drawn to the quick rewards of faster transactions. Small and mid-market FIs must instantly extinguish these threats and secure their financial ecosystems with real-time fraud detection and interdiction. When safeguarding customer trust and financial integrity, it's the decisive action in real time that defines the true modernity of a bank's defenses.

Eric Tran-Le is vice president, head of Actimize Premier for NICE Actimize.

Past Issues

DECEMBER 2023
2024 banking outlook »

NOVEMBER 2023
Priorities in talent and professional development »

OCTOBER 2023
Marketing strategies for the digital age »

SEPTEMBER 2023
The insights of data and analytics »

AUGUST 2023
Creating new opportunities through open banking »

STAY TUNED FOR

FEBRUARY 2024
Strategies for customer growth, deposits & retention

MARCH 2024
Evolution of banking branches

BAI Banking Strategies
EXECUTIVE REPORT

Safeguarding against fraud

JANUARY 2024

BAI POWERING SMART DECISIONS.