BAI Banking Strategies

EXECUTIVE REPORT

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



JANUARY 2023

BAI POWERING SMART DECISIONS.

In this issue

3 **The art and science of fraud prevention**
AI and machine learning add speed and power to fraud-prevention efforts, but skilled people are needed for the judgment calls.

6 **Deposit accounts in the fraud crosshairs**
The rapidly growing trend, driven by powerful technology, combines new (P2P payments) and old (check washing) into a vexing mix.

9 **Banks need to be ready for better deep fakes**
The technology is getting better for both audio and video, which will create new use cases for scamming banks and their customers.

12 **Fraud detection is faster, yet still too slow**
The goal for banking institutions is not only to detect fraud in as close to real time as possible, but also to anticipate the bad guy's next move.

15 **Striking a balance between fraud and friction**
How identity-verification solutions can streamline workflows and build consumer trust.

18 **Managing the risks and rewards of faster payments**
Small and midmarket financial institutions need layered approaches to fraud prevention that also support a differentiated banking experience.

21 **Mitigating the challenges of 'piggybacking'**
Purchasing an authorized user tradeline is not technically illegal, but it abuses regulatory intent and elevates credit risk for banks.

24 **Protection from check fraud in a digital world**
High-tech printers, specialized ink and other advances can add security to a payment method still embraced by many businesses of all sizes.



Fraud prevention today is about much more than automation

BY TERRY BADGER, CFA
tbadger@bai.org

The full extent of banking losses from fraud have yet to be tallied for 2022, but I don't feel like I'm out on much of a limb in speculating that the trend line will continue moving as it has for years: Up and to the right.

And those losses on their own don't reflect the total cost to banks and credit unions. A November 2022 report from LexisNexis Risk Solutions estimates that every dollar lost to bad actors actually costs financial services firms $4.23—this 4X+ multiplier is up roughly 16% from 2020.

In the first BAI Executive Report of 2023, we examine where things stand with fraud protection and how it can be done more efficiently and effectively.

Our lead article from contributing writer Ed Lawler explores the evolving role of the living and breathing in what has largely become a technology-forward fight against fraud.

He speaks with several thought leaders in the field who agree that, while anti-fraud efforts will continue to be largely reliant on automation and other cutting-edge capabilities, human brainpower and intuition are more important assets than ever. As one points out, "Technology tools can only get you so far. … We need people with the right mindset and the right art to connect the dots."

Strong data science skill sets supplement the curiosity and creative thinking by fraud-risk managers working to get into the heads of fraudsters and figure out ahead of time how they would try to beat the system.

A growing number of headlines about scams involving peer-to-peer payments fraud have directed more regulatory focus toward that corner of the fintech world. Contributing writer Dawn Wotapka offers insights on P2P fraud, along with other persistent forms of criminal behavior occurring at the consumer level.

One of the key takeaways from her reporting is that would-be fraud perpetrators no longer need that much technical skill to pull off their scams. "Social media is full of 'how-to' videos and tools on how to commit fraud," one industry expert tells her, while another adds, "We should never underestimate today's criminals."

And as if fraud perpetrated by real people weren't challenging enough, financial institutions also need to worry more about the growing proliferation of deep fakes as the technology is getting better in both audio and video formats.

For this month's Q&A, I speak with Vijay Balasubramaniyan, CEO at the fintech firm Pindrop, about his observations in the deep fake space and what those being targeted can do about it. He says banks and credit unions currently face the greater threat from audio deep fakes, which are particularly close to the genuine article: In a test created by his company, barely more than half of participants were able to distinguish between a real person's voice and a fake version of that voice.

Also in this month's Executive Report:

» **Digital fraud is front and center in 2023:** Greg Kanevski from ServiceNow examines online fraud, which he believes will take on even greater urgency this year. The goal for banks and credit unions, he says, is to detect fraud in real time while also predicting a fraudster's next move to try to head it off.

» **Striking a balance between fraud and friction:** Christina Luttrell from GBG Americas discusses some of the findings from her company's recent study on consumer experiences and expectations regarding digital identity fraud. A persistent issue is optimizing the trade-offs between protecting customers and providing a satisfying user experience.

» **Managing the risks and rewards of faster payments:** Eric Tran-Le from NICE Actimize tells us that the global pursuit of ever faster payment capabilities to meet consumer expectations is posing a range of fraud prevention challenges for regional banks, community banks and credit unions.

» **Mitigating the challenges of 'piggybacking':** Jason Kratovil from SentiLink writes about the growing market for buying and selling legitimate tradelines as a way for individuals with low credit scores to improve their credit report. This action is often a form of first-party fraud that leads to higher charge-off losses.

» **Protection from check fraud in a digital world:** Nathan Holstein from TROY Group reminds us that paper checks are still a relevant payment method for many businesses, and that the industry shift toward digital has led to more focus by fraudsters on this lower-tech channel.

We hope this Executive Report provides value that your institution can put to work in protecting itself from the many fraud risks you face. Feel free to email me to let me know what you think.

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



The art and science of fraud prevention

AI and machine learning add speed and power to fraud-prevention efforts, but skilled people are needed for the judgment calls.

BY EDMUND LAWLER

Inquisitiveness. Tenacity. A strategic mindset. Analytical thinking. An aptitude for technology. Problem-solving ability. Creativity under pressure.

Does your fraud-detection bot powered by artificial intelligence come with those characteristics?

BAI spoke recently with four thought leaders in the fraud detection and prevention field who agree that automation is invaluable—but human intuition is more essential than ever in the fight against fraud at financial services organizations.

Kevin Sanchez, senior vice president and head of U.S. Bank's digital financial crimes team, says AI in fraud-risk management continues to evolve in ways that help human fraud teams get better at what they do.



KEVIN SANCHEZ
U.S. BANK

"AI and machine learning enable us to take some of the human artistry and apply it through a scientific lens to help us be more efficient in managing fraud risk and delivering the customer experience," he says.

Sanchez, who has led the team at the Minneapolis-based bank since 2020, looks for several qualities in hiring team members. "First, you need someone with a strategic mindset," he says. "It's critical that a fraud-risk manager is able to optimize fraud-risk management on one side of the coin and ensure that we are optimizing the customer experience on the other."

He also looks for candidates who have enough technical understanding to recognize potential vulnerabilities in a technology about to be deployed. "A good fraud-risk manager has a curious

"AI and machine learning enable us to take some of the human artistry and apply it through a scientific lens to help us be more efficient in managing fraud risk and delivering the customer experience."

KEVIN SANCHEZ
U.S. BANK



ASH KHAN
BMO FINANCIAL GROUP

mindset and can think like a fraudster: How would they try to beat the system?"

And Sanchez likes candidates who think analytically. "There is a lot of problem-solving, a lot of troubleshooting," he notes. "You need someone who can analyze data; who can draw some hypothesis or conclusions out of the data to solve challenges that will emerge and then fight the fire."

But finding that kind of talent within the financial services field can be challenging. "There's a lot of highly skilled fraud-risk managers outside of payments or financial services. Because they have that ingrained technical knowledge and expertise, they may very well be able to fit seamlessly into a financial services role."

> **"It's a balance of art and science. ... We can't rely solely on technology to solve our fraud problems. Technology tools can only get you so far. The human element is critical. We need people with the right mindset and the right art to connect the dots."**
>
> **ASH KHAN**
> BMO FINANCIAL GROUP

Ash Khan, head of enterprise fraud management for BMO Financial Group, says it's not just the members of his team who are responsible for preventing fraud at the Toronto-based bank. For example, BMO's fraud foundational training program allows employees to visit the bank's portal to watch videos on fraud-related topics such as account takeover.

"All employees have a role in preventing fraud," he says. "That's because they are the ones who interact on a daily basis with customers."

Khan says most candidates for his team come from financial services, "but we do hire people from other disciplines. I have hired quite a few people who don't come from traditional banking, but they have strong data science skill sets. ... We have also hired people from our call center or customer service reps from the branches. They understand customer interactions and how things work at the branch level, as well as the products and services we offer."

So is fraud prevention an art or a science?

"It is a balance of art and science," Khan says. "We are constantly working to strike that balance. We can't rely solely on technology to solve our fraud problems. Technology tools can only get you so far. The human element is critical. We need people with the right mindset and the right art to connect the dots."

Canh Tran, co-founder and CEO of Chicago-based Rippleshot, which uses AI and machine learning to protect financial institutions from card fraud losses, naturally has a soft spot for technology.

"Technology can save users a lot of time through automation or analysis," Tran says. "It can go through millions of transaction records and look at fraud and tell you what the trends are. That would



CANH TRAN
RIPPLESHOT





KEVIN EACK
BRANNAN GROUP

> **"A good analyst or an effective fraud investigator understands that the anomaly has only drawn their attention to a particular area. Then the human takes over and studies what's really going on with this behavior."**
>
> **KEVIN EACK**
> BRANNAN GROUP

take a human a very long time to do. That allows the manager to spend more time strategizing fraud-prevention measures."

But, he adds, "Cultivating talent is just as important as the latest technology. You need both technology and talent. Technology can be a game changer and can solve a lot of problems. But it can't be done alone. It still has to be decided by and operated by humans."

Kevin Eack, who heads the Brannan Group, a Peoria, Ill.-based security consultancy, believes an effective bank fraud preventer "needs a curious and investigative mind that says: 'Something doesn't look right here.' I come from a police background, so I'm tempted to say they need to think like a cop."

Eack was a senior executive with the Illinois State Police and served two tours of duty with the FBI, most recently as one of two fellows to then-FBI Director Robert Mueller specializing in counterterrorism. He also headed a financial crime team for State Farm Bank from 2011 to 2015.

Bots and other fraud-detection technologies are adept at identifying anomalies in accounts that might point to suspicious activity, he says.

"But those kinds of technology advances only take you part of the way. A good analyst or an effective fraud investigator understands that the anomaly has only drawn their attention to a particular area," he says. "Then the human takes over and studies what's really going on with this behavior. Is it fraud? Is it something worth bothering the customer about? Or could it just be a little change in pattern?"

As an example, he cites an analyst who detected a fraudster's handiwork when an affluent couple's



large home equity line of credit was being rapidly drained.

"Suddenly, $100,000, $150,000 and $200,000 is getting moved out of the account, all within a 24-hour period," Eack says. "The analyst tried to call the customer to verify it was them moving the money."

But the fraudsters had rerouted the couple's phone because they knew the bank would call to verify the movement of the money. The person who answered the couple's rerouted phone number was an actor who assured the analyst that all was well and that the funds were being withdrawn to pay for a home-improvement project.

The fake customer, however, had an accent that didn't match the customer's profile, raising a red flag for the analyst, who went online and dug up some old information about the customer, including a different phone number. The analyst reached the wife, who said that neither she nor her husband had withdrawn the money.

"It's that sort of digging, those extra steps, where the human makes a big difference because technology is only going to draw your attention to something that is different," Eack says. "It's not going to fully investigate it."

Edmund Lawler is a BAI contributing writer.

Deposit accounts in the fraud crosshairs

The rapidly growing trend, driven by powerful technology, combines new (P2P payments) and old (check washing) into a vexing mix.

BY DAWN WOTAPKA



The COVID-19 lockdowns ushered in a golden era for digital activity: We all worked, socialized and banked from behind a keyboard. Criminals got in on the action, increasing the work for banks and financial institutions already battling a multitude of fraud issues.

"There are continued fraud threats that we do not see abating in 2023," says Jen Martin, head of enterprise fraud services for KeyBank. "Scams, identity theft, new-account fraud and checking account fraud all have been elevated throughout the year and will continue for the foreseeable future."

Much of the fraud plaguing U.S. banks and their customers emanates from criminal organizations based outside the country. "I believe that the globalization of fraud through technology and social media, in addition to what we continue to manage in our local communities, will continue to advance and evolve next year and beyond," Martin says.

A hot area for fraudsters is peer-to-peer (P2P) fraud, which has surged in popularity as consumers increasingly send money almost instantly using tools that include Zelle and Venmo. Since 2017, Zelle has facilitated more than 5 billion transactions totaling more than $1.5 trillion. In the second quarter of 2022 alone, year-over-year payment values increased by 29%, while payment volume increased by 27%. While the vast majority of that usage is secure and scam-free, the systems are like candy to scammers.

Meanwhile, NICE Actimize has seen a 63% increase in attempted P2P fraud in 2021 versus 2020, says Glenn Fratangelo, head of strategy and marketing for fraud and authentication management. No one will be surprised if that number climbs again in 2022.

And even in a digital-first age, check fraud continues. "Criminals continue to look to exploit the weakest link, checks being one of these channels," Fratangelo says, pointing to his company's internal data showing a 106% year-over-year increase in check fraud from 2020 to 2021 and an additional 30% increase in the first nine months of 2022. When you consider that there's been an overall decline in check usage, the calculation becomes more dramatic. "Fraud in the channel is outpacing total transactions, indicative of a payment channel currently under siege by criminals," he says.

Check washing may be one of the oldest tricks in the book, but it is making a comeback as fraudsters obtain a paper check and alter the payee, the dollar amount or both. To the untrained eye, the check looks valid. One issue feeding this rise is that municipal governments and small businesses are being hit more frequently by ransomware or encryption events, says Howard Globus, CEO of IT On Demand and a self-described cybersecurity evangelist. "As systems are compromised or



JEN MARTIN
KEYBANK

unusable, these organizations have switched over to paper checks to pay vendors and recipients of program funds.

"Sometimes it's because there is a belief that paper checks are safer. Other times the systems are so damaged that accounting software will not run or banking partners will not accept electronic fund transfers until their systems are certified safe. … Unfortunately, the increase in paper checks in circulation increases opportunities for fraud."

One doesn't have to be particularly tech-savvy to be a fraudster these days. "Social media is full of 'how-to' videos and tools on how to commit fraud,"

> **"Social media is full of 'how-to' videos and tools on how to commit fraud. No longer is fraud specific to a certain criminal; information on how to commit fraud is widely available and easier to find than ever before."**
>
> **JEN MARTIN**
> KEYBANK

Martin says. "No longer is fraud specific to a certain criminal; information on how to commit fraud is widely available and easier to find than ever before." And as soon as one scam is caught, a new one emerges. "We should never underestimate today's criminals," Fratangelo says.

For financial institutions, fighting all fraud requires the right balance between consumers' demand for speed, younger users' growing disdain for passwords and communication fatigue. Banks are working to catch fraud instantly, but that can involve communication with a customer—and most consumers juggle hundreds of email messages, texts and social media notifications, making it harder for critical messages to cut through the clutter.

"It is a 'Catch-22' for financial institutions: 98% of all text messages are read by the recipient versus 20% for emails," says Richard Dedor, vice president



of digital marketing for Chatsworth, California-based Premier America Credit Union. "With the rampant expansion of text fraud, financial institutions must be extra careful about their marketing and message strategies to ensure they are educating their users on how to distinguish authentic communications from the fraud."

Combating check fraud "requires a holistic and omnichannel approach," Fratangelo says, adding that financial institutions need to update their current check-fraud systems to a single solution powered by AI that can detect anomalous



behaviors and transactions. Also helpful is detection analytics enriched with both check-image analysis and data from the dark web on compromised checks.

KeyBank, for one, is breaking down the industry's traditional silos to create a solution. "We are collaborating across the bank—fraud, risk, product and technology partners are all coming together against a common enemy," Martin says. "A positive outcome of the past year is a greater understanding that there is not just one department or tool that can stop fraud. Real fraud prevention and mitigation requires subject matter expertise and understanding across many functional areas to ensure there are not opportunities for fraud."

Globus says customers can also play a role. For example, they can pick up mail as soon as it is delivered, use a lockbox instead of an easily accessible mailbox, check bank accounts daily to spot fraud, use sophisticated biometrics to unlock phones and employ multifactor authentication. "The more steps you can put in place to block access to apps on your phone, the safer your data is and the more likely you are to be able to protect yourself," he says.



HOWARD GLOBUS
IT ON DEMAND



RICHARD DEDOR
PREMIER AMERICA CREDIT UNION

"The more steps you can put in place to block access to apps on your phone, the safer your data is and the more likely you are to be able to protect yourself."

HOWARD GLOBUS
IT ON DEMAND

To be sure, no single player can do this alone. "The global financial crimes and fraud problem," Martin says, "is well beyond any one financial institution to solve by ourselves or as an industry."

Dawn Wotapka is a BAI contributing writer.



Banks need to be ready for better deep fakes

The technology is getting better for both audio and video, which will create new use cases for scamming banks and their customers.

BY TERRY BADGER, CFA

Much of the fraud assailing the financial services industry falls into the category of someone pretending to be someone else. That deception can be easier to pull off when the scammer can look like or sound like their victim.

Enter deep fakes, which have been around for some years now and, as technology has advanced, have improved in quality. It hasn't reached the point where the phony version is indistinguishable from the genuine article, but that gap is narrowing.

This is particularly true for audio deep fakes. Vijay Balasubramaniyan, CEO at the fintech firm Pindrop,



says his company put together a test where participants listened to two pieces of audio and had to select which one was real and which was fake. Only slightly more than half of the participants chose correctly.

We recently spoke with Balasubramaniyan about how deep-fake technology is being used against banking institutions and what those targeted can do about it.

The interview has been edited for length and clarity.

BAI: What can you tell us about how deep fakes are being used against banks in the U.S.?

Vijay Balasubramaniyan, Pindrop: We're starting to see attacks on the U.S. banking side where deep fakes are being used for a couple of things. The biggest bucket of fraud that most of these organizations see, including banks, is business email compromise. We're starting to see a form of that with phone calls where they call a bank and say, "Hey, I need to wire this money out because I have this really important deal that I need to use it for." They impersonate important people at organizations like the CEO or the CFO. A second use is for account openings. Using deep-fake technology, you can actually create a synthetic identity that has the likeness of a person, including a deceased person, and start doing transactions on that person's behalf.



VIJAY BALASUBRAMANIYAN
PINDROP

> "Using deep fake technology, you can actually create a synthetic identity that has the likeness of a person, including a deceased person, and start doing transactions on that person's behalf."
>
> **VIJAY BALASUBRAMANIYAN**
> PINDROP

Can you give us a sense of how much success the deep fakers have been having in their efforts to scam bankers?

The biggest one is a $35 million bank heist, and it happened across the UAE and Hong Kong, where a branch manager was asked to wire $35 million on behalf of a client. Across a wide variety of accounts, he actually wired this $35 million. This started getting attention in the U.S. because there was a bank in the U.S. where about $400,000 of that $35 million got wired into a fake account.

Many in the fraud world are good with technology—is this a necessary skill for creating and using deep fakes?

Sometimes they're using just basic deep-fake technology, but they're using it in tandem with their old techniques. The scary thing is, because a lot of basic-level deep fakes are not yet so prevalent, you have no reason to believe that it's actually a deep fake on the other end. These guys are combining the deep fake with a sense of urgency to convince people on the other end of the call that it is the real person—"I'm the CEO of the company and I'm on a plane, so I'm going to be out of pocket for the next

two hours, but I want the money by the time I land or we will lose the acquisition." In one deep-fake case where millions of dollars were wired, the CEO isn't a very public persona, but the fraudsters hacked into their system to get audio from internal communications, and they used that to create a deep fake.

What advice do you give clients regarding how they can better protect themselves and how they can better protect their customers from this technology?

One is to adopt technology that can detect deep fakes so you can determine when a customer is being deep faked, especially when he's asking to do a million-dollar wire transfer even when a million-dollar transfer is natural. This can also help a bank make sure accounts being opened are not deep-fake accounts or ones with synthetic identities. There is also risk when a bank is hiring employees in this remote work environment—they need to make sure those employees are who they say they are and not synthetic employees created using deep-fake technology. We ask them to look at each of these areas in order to make sure that they understand the impact that deep fakes could have. We also talk about advising customers to do similar checks when they get a call from someone claiming to be from the bank to make sure they're not being scammed.

How do you think the use of this technology might change in the coming years?

The thing that worries me the most is, at least as far as banking is concerned, there don't seem to be very many reasons why deep fakes are going to be used for good. The only potential reason is when organizations are trying to create a virtual assistant that represents them. In that particular case, it's a synthetic voice. It's not quite a deep fake. But



"These newer mechanisms are definitely very customer-friendly, but how are you making sure that it's the customer on the other end? You're going to see more and more of synthetic identities being created in order to open up new accounts as well as take over accounts, and this is where banks have to be very vigilant going forward, especially as they increase the number of ways in which they interface with customers."

VIJAY BALASUBRAMANIYAN
PINDROP

in terms of how these organizations are starting to deal with customers, traditionally they would talk over the phone. Now they're starting to talk over Zoom or WhatsApp. These newer mechanisms are definitely very customer-friendly, but how are you making sure that it's the customer on the other end? You're going to see more and more of synthetic identities being created in order to open up new accounts as well as take over accounts, and this is where banks have to be very vigilant going forward, especially as they increase the number of ways in which they interface with customers. Another thing



I worry about is misinformation. An example might be that a fake video of the CEO or the CFO of a bank is made in which they say the earnings call next week is going to be terrible because we missed our numbers. I think we're going to see more of that because that's an easy way to try to influence something like a stock price and then take advantage of the false information.

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



Fraud detection is faster, yet still too slow

The goal for banking institutions is not only to detect fraud in as close to real time as possible, but also to anticipate the bad guy's next move and stop it.

BY GREG KANEVSKI

For generations, banks feared robberies that would put their tellers at risk, and then check fraud became the biggest threat. Now, a far larger concern is online fraud. Increasing activity in this area, which many industry watchers consider the new normal, is increasingly weighing on the bottom line, making detection and prevention an even stronger focus for the banking industry in 2023.

While online financial fraud is certainly not a new problem, it exploded during the global pandemic, when consumers turned to digital banking and changed their transaction behavior. As consumers increasingly used laptops and smartphones for banking needs, instances of fraud increased. How big is the problem? Information giant LexisNexis found that every dollar lost to fraud costs financial institutions four times that amount, and this multiplier has further increased since COVID-19 swept the globe.

Digital fraud may seem simple, but it comes in multiple complex forms. Most people know about identity theft and phishing scams, which use fake email and/or deceptive websites to obtain account information. But fraud can also be more intricate, involving everything from installing malware to entirely taking over someone's account. In addition to financial damages, the fraud disrupts companies and, in the worst cases, upends consumers' lives.

The banking industry—by which we mean traditional and nontraditional banks, fintechs and mortgage companies—is working hard to stay ahead of these nefarious actors. The goal is not only to detect fraud in as close to real time as possible, but also to anticipate fraudsters' next move with the goal of heading it off.

Most people know about identity theft and phishing scams, which use fake email and/or deceptive websites to obtain account information. But fraud can also be more intricate, involving everything from installing malware to entirely taking over someone's account. In addition to financial damages, the fraud disrupts companies and, in the worst cases, upends consumers' lives.





If you think this should be easy to fix, think again. Remember the game of Whac-A-Mole? Here's what Accenture had to say: "Even as financial institutions and businesses adopt the latest strategies to make digital payments more secure, the nature of digital fraud continues to evolve. The new-age hacker is using more sophisticated, innovative ways to obtain valuable customer information and login credentials to hack into accounts."

Consumers have little patience for the headaches and stress these fraudsters create. They expect financial institutions to understand their patterns and habits and know when something seems amiss. But considering the sheer number of transactions every second, this is a tough demand to meet.

In response to consumer expectations, the industry is tapping artificial intelligence to help. Each institution's algorithms are based on its own specific risk tolerances and customer base. A money-center bank, for example, might expect a high number of customers to travel globally, while a smaller regional bank might flag a transaction from overseas because its customers are more likely to stay regional.

When working to detect fraud, banks have to combine an understanding of customer nuances with the utmost speed. Every second spent responding to a potential fraud alert costs money. And AI can't do it alone. Humans have to review potential issues and decide whether to act. Unfortunately, many institutions have disconnected systems and staffers, hindering their ability to act quickly.

Consider a fraud prevention group that has its own system. After receiving an alert, the fraud preventers send the alert to another team for action. Whoever talks to the customer may use yet another tool. This back and forth takes valuable time, an inefficiency the industry is working to remedy. We're seeing more examples of companies merging groups to speed up responses as customers get more savvy—and their expectations continually increase.

Smart institutions automate low-value tasks, such as detecting a potential problem based on prior activity, but have a human step in when needed. Each bank or credit union will set its own criteria for when to involve an employee—is it the value of the transaction itself? Or the value based on the customer's risk or exposure?



In response to consumer expectations, the industry is tapping artificial intelligence to help. Each institution's algorithms are based on its own specific risk tolerances and customer base. A money-center bank, for example, might expect a high number of customers to travel globally, while a smaller regional bank might flag a transaction from overseas because its customers are more likely to stay regional.

An emerging question is how to balance this while protecting the bottom line and consumer data. What if fraud puts a customer's account in the negative, incurring overdraft fees? Who pays for that? The regulators will expect the bank to reverse these fees. A real problem here is yet another group has to be engaged, and it costs more time and money.



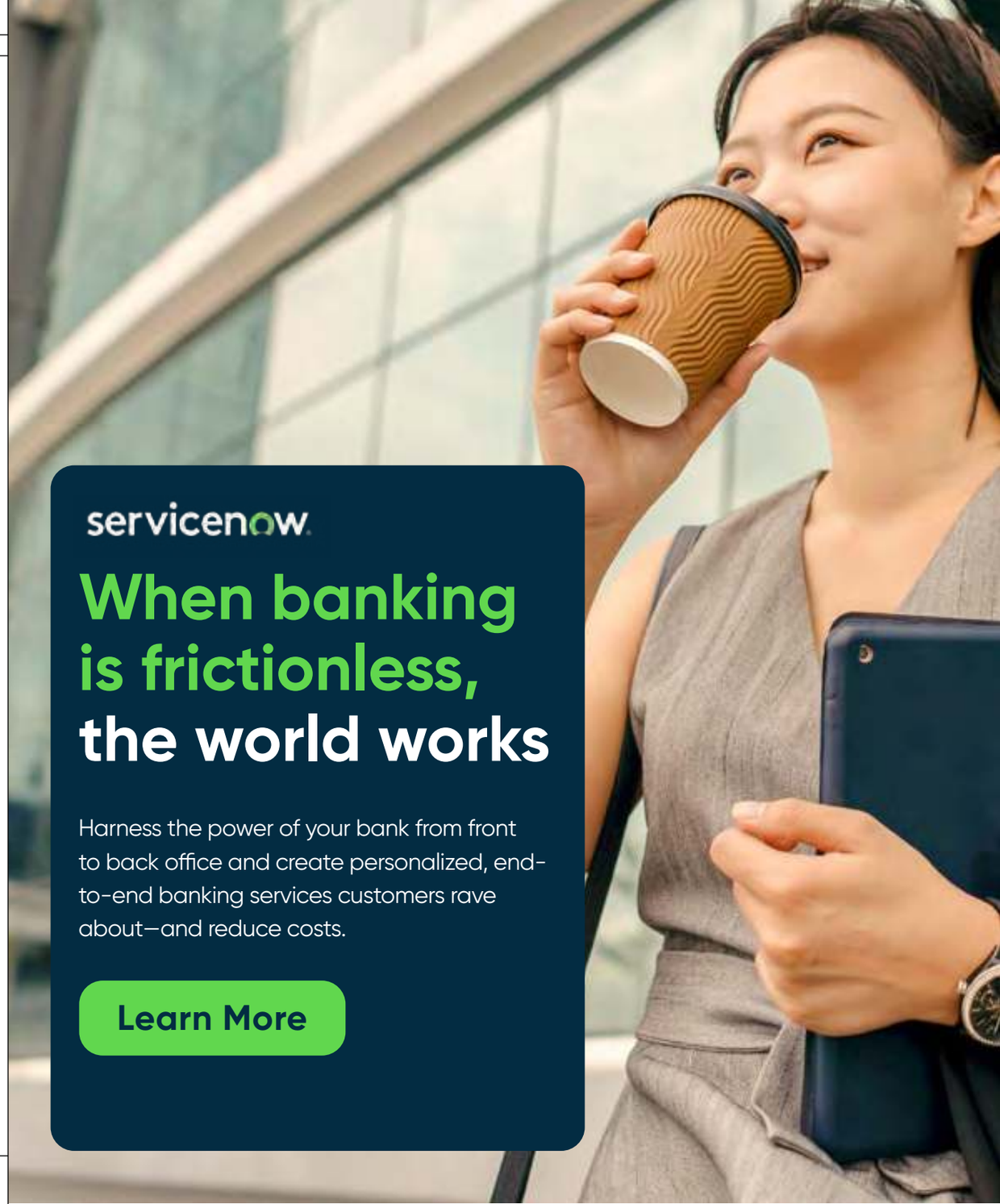
Regulators are also pushing the industry to look at the customer holistically. They're pushing for combined reporting and information on how these institutions are responding to all customer classes equally. This is difficult, given the way fraud and disputes are traditionally managed, with different teams, multiple tools and different processes.

Regulators are also pushing the industry to look at the customer holistically. They're pushing for combined reporting and information on how these institutions are responding to all customer classes equally. This is difficult, given the way fraud and disputes are traditionally managed, with different teams, multiple tools and different processes.

Meanwhile, banks are finding new ways to uncover fraudulent activity. Spotting fraud on a customer's account is important, but so is catching abnormalities in peer groups. For example, AI is being used to flag accounts with unusual credit/debit card activity at a broader level (i.e., by batches, customer groupings, merchants, etc.). In cases like this, detecting fraud benefits not only the customer but also the financial institutions, commercial markets and the larger ecosystem.

Banks of every size in every region need to tackle this issue. They recognize that customer behaviors have changed. They realize that many more transactions are digital. They also know this is not a one-and-done issue. They're looking into the future because no one expects digital transformation to stop. And as long as consumers are banking online, bad actors will keep entangling financial institutions in a cat-and-mouse game.

Greg Kanevski is head of global banking at ServiceNow.





Striking a balance between fraud and friction

How identity-verification solutions can streamline workflows and build consumer trust.

BY CHRISTINA LUTTRELL

There's no denying that fraud is on a disastrous upward trend. One report from the U.S. Senate highlights data from four major banks that tallied nearly 200,000 instances of fraud in 2021 and the first six months of 2022, with a cumulative estimated cost of over $200 million.

While financial institutions are keenly aware of the impact of fraud, they need to start considering the lasting effects these threats have on consumer trust. IDology's 5th Annual Consumer Digital Identity Study found that 56% of consumers expect fraud attempts to increase, up from only 38% in 2021.

As fraud risk continues to increase, consumer needs and expectations are reaching new highs. Security and ease are now critical components of consumers' digital interactions. Identity-verification solutions that analyze multiple diverse data sources provide visibility into

cross-industry fraud intelligence and allow financial institutions to strike a needed balance between safety and convenience.

Institutions need to facilitate trust as a fundamental part of any workflow they provide to consumers. Losing consumer trust when an experience feels insecure or when a digital interaction fails to meet a consumer's expectations can have a significant impact on an institution's ability to be competitive. IDology's survey found that 37% of consumers say they've abandoned efforts to sign up for a new online account because they don't trust the process.

Additionally, a lack of trust causes consumers to be more careful about where they share their personal information. Close to two-thirds of those surveyed report being selective about doing business with companies that require personally identifiable information. Consumers are also generally motivated to move on if it means a better experience, with 70% of consumers surveyed saying they are actively considering switching financial services providers.

In a competitive market, building trust can be an essential differentiator in making or breaking consumer interactions. Given that consumers are less trusting and require more assurance, especially during the "trust moments" associated with new-account creation, institutions must



Losing consumer trust when an experience feels insecure or when a digital interaction fails to meet a consumer's expectations can have a significant impact on an institution's ability to be competitive. IDology's survey found that 37% of consumers say they've abandoned efforts to sign up for a new online account because they don't trust the process.



be able to quickly verify legitimate identities in a less invasive and more transparent way. This can be accomplished with flexible and data-diverse verification technology, which empowers institutions to ensure that onboarding is quick and easy and that step-up verification methods, such as knowledge-based authentication or ID document verification, are used only when necessary.

HELPING CONSUMERS PROTECT THEMSELVES

A lack of trust brought on by fraud poses a clear challenge to institutions, but fraud also causes lasting effects. Consumers reported a variety of downstream fraud attacks after discovering their identity was stolen. Financial-related fraud topped the list, with illicit money transfers from a bank account, card-related fraud and mobile-based attacks being the most common.

To make things more challenging for institutions, they can't rely on consumers to act even if it is in their best interest. After discovering their identity was compromised, only 16% of consumers signed up for an identity protection service, 17% signed up for a credit monitoring service and 30% turned on fraud alerts through their financial provider.

Consequently, institutions are uniquely positioned to protect a consumer who is looking for more security but is also mostly unaware of what actions to take. Only 17% of survey respondents said they

Among survey respondents, 76% said that knowing an online company is using advanced identity verification would influence them to use the company's services. 32% said that a quick and easy process is the most important factor in opening an account, and 45% showed a strong dislike for companies that require additional security checks. In other words, consumers value security, but they demand convenience.

knew what synthetic identity fraud is, a fraud type that most institutions are likely well aware of. With better identity-verification technology in place, financial institutions can build trust with low-friction workflows while preventing fraud from entering their enterprise.

OFFERING SECURITY AND CONVENIENCE

Financial institutions are continuously challenged to stay one step ahead of fraud, but they're also challenged by consumer expectations. In a highly digitalized environment, consumers expect seamless interactions that are as secure as they are helpful. With modern identity-verification technology, institutions can meet these challenges head-on.

Among survey respondents, 76% said that knowing an online company is using advanced identity verification would influence them to use the company's services. However, 32% said that a quick and easy process is the most important factor in opening an account, and 45% showed a strong dislike for companies that require additional security checks. In other words, consumers value security, but they demand convenience.

To satisfy these seemingly conflicting sentiments, financial institutions must provide consumers with secure digital experiences that deter fraud without adding unnecessary friction. Intelligent identity-verification technology can strike the right balance between fraud and friction. Correctly implementing automated, multi-layered identity verification can streamline 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.

Christina Luttrell is chief executive officer of GBG Americas.

Approve More Customers **Without Increasing** Friction or Fraud

Industry Leaders Choose IDology:

4,000+ Customers

2,500+ Banks and Credit Unions

30+ of the Top 100 Financial Institutions

The IDology Difference:

- Drive new accounts with superior locate and approval rates
- Deter fraud with the leading multi-industry fraud network
- Decrease costs through reduced manual review process



Visit IDology.com to learn more.

IDOLOGY a GBG company

Innovative solutions to streamline customer acquisition, deter fraud,

Managing the risks and rewards of faster payments

Small and midmarket financial institutions need layered approaches to fraud prevention that also support a differentiated banking experience.

BY ERIC TRAN-LE

Instant access to funds is the new nonnegotiable for today's consumers and businesses.

Approximately 70% of consumers indicate that faster payment capabilities are an important factor in their satisfaction with financial institutions. Likewise, businesses are emphasizing faster and real-time payment capabilities in their banking decisions: 21% of small and medium-sized businesses express extreme interest in RTP settlement, and about 75% of medium- and large-sized businesses plan to incorporate faster payment capabilities into their future banking relationship commitments.

On a global scale, the trend toward faster and real-time payments was accelerated by the pandemic and the associated uptick in digital activity. This environment fueled technology advancement and accessibility, fundamentally influencing how consumers and organizations view instant payments and establishing the ideal conditions for complex fraud.





For regional banks, community banks and credit unions, the struggle to implement, operationalize and monetize robust fraud prevention can overshadow the opportunities awarded by delivering RTP functionality.

Small and midmarket FIs face a once-in-a-generation crossroads: Either seize the competitive advantage provided by RTP and adopt the requisite advanced fraud prevention, or risk becoming a cautionary tale to peers.

SLOW ADOPTION OF RTP

Now that consumers are adopting third-party mobile payment apps and mobile wallets, they expect similar transaction experiences from their financial institutions.

Various research shows that, for a large percentage of consumers, their decision on opening a new account will factor in the availability of real-time payments. Yet small and midmarket FI adoption of RTP has been sluggish; for example, just 16% of surveyed credit unions currently offer RTP solutions, and 23% are uncertain about future plans to implement RTP capabilities.

Among these financial institutions, hesitation to embrace RTP is often attributed to the intricacy of integrating new types of payments, the challenges of managing RTP rails and the absence of a federal mandate to implement those rails.

FIs that provide RTP capabilities can experience increasing transaction volumes. Within six weeks of connecting to a real-time payment rail network, one leading credit union witnessed a 45% rise in RTP network transactions and a 61% increase in the number of members receiving transactions.

However, FIs that provide RTP capabilities can experience increasing transaction volumes. Within six weeks of connecting to a real-time payment rail network, one leading credit union witnessed a 45% rise in RTP network transactions and a 61% increase in the number of members receiving transactions.

Another primary concern regarding adoption of faster and real-time payment capabilities is vulnerability to fraud. RTP represents an efficient vehicle for fraudsters to cash out via fraud tactics such as account takeover, authorized push-payment scams, peer-to-peer fraud and synthetic identity fraud.

The scale and velocity of fraud attacks and the industrialization of fraud have exposed weaknesses in static fraud-prevention approaches, existing fraud controls and rules-based fraud-prevention systems.

Financial institutions must contend with a variety of fraud-prevention challenges posed by faster and real-time payments:

- *They are exposing their infrastructures to third-party applications to facilitate payment initiations from different instant applications.*
- *When customers use third-party applications, there's no end-point detection.*
- *There are obstacles to gaining sufficient data and information to ensure risk engines can perform effectively with the FI's systems.*
- *Fraudsters can coerce customers into using new platforms on which transactions are authenticated or initiated in the third-party application outside of the bank's control.*

With the FedNow Service joining the U.S. payments ecosystem in 2023, small and midmarket banks have an incentive to develop a strong RTP strategy and a corresponding framework for advanced fraud prevention.

HOW ARTIFICIAL INTELLIGENCE CAN HELP

Small and midmarket FIs are under extreme pressure to modernize their fraud-prevention solutions. Data silos, lack of contextual insight and fragmented point solutions hinder decision-making and risk management, putting the organization and its customers at greater risk.

For example, credit unions are particularly susceptible to online fraud as a result of vulnerabilities from manual reviewing processes, legacy fraud-prevention systems, insecure email networks and leaked personnel credentials. These exposures can lead to the risk of attacks that can be worth as much as $190,000 for small credit unions and $1.2 million for large credit unions.

Banks and credit unions should adopt a holistic, multidimensional approach to fraud management built on artificial intelligence, machine learning, high-quality data and behavioral analytics. These capabilities work in conjunction to:

- *Derive patterns from copious quantities of diverse data and generate pertinent, real-time insights that improve business processes and operations, decision-making, and the customer experience.*
- *Detect aberrant behaviors, enabling financial institutions to continuously update fraud-prevention approaches that align with the scale, complexity and pace of fraud.*
- *Anticipate and minimize risk exposure and embed effective safeguards into services and products.*
- *Support the operational and technological convergence of measures to combat fraud and money laundering for enhanced cost efficiency and analytics insights.*
- *Promote operational and business agility amid disruption, data breaches, the progression of digitalization and the evolving payments and threat landscape.*
- *Explore innovative use cases for monetizing RTP, including P2P, account-to-account, person-to-business and business-to-business payments.*
- *Contextualize fraud threats and accurately detect fraud.*

Intelligent capabilities should be complemented by best practices, such as customer education on how RTP works and evolving fraud and scam tactics, and employee awareness of potentially fraudulent authorized push payments.

Fraudsters are investing in smart technologies and processes that perpetuate and expedite sophisticated fraud at scale. Community banks, regional banks and credit unions must respond with modern, layered approaches to fraud detection and prevention that simultaneously support a differentiated digital banking experience.

Small and midmarket financial institutions must act quickly to solidify their place within the faster and real-time payments market and capitalize on competitive opportunities.

Eric Tran-Le is vice president and head of Actimize Premier at NICE Actimize.

NICE Actimize
Know More. Risk Less.

Xceed

Combat fincrime with our all-in-one FRAML solution.

Designed for today's mid-market, regional, and community banks, and credit unions, **NICE Actimize Xceed** offers real-time, **complete Fraud and AML coverage** on a single cloud-native platform.

niceactimize.com/**xceed**



Mitigating the challenges of 'piggybacking'

Purchasing an authorized user tradeline is not technically illegal, but it abuses regulatory intent and elevates credit risk for banks.

BY JASON KRATOVIL

Plug "buy a tradeline" into any search engine, and the results might be surprising. Instead of landing in some unsavory corner of the "dark web," you'll find fully realized, highly sophisticated storefronts on par with many other online marketplaces.

These are not scams. Right there, in the clear light of day, a person can purchase access to another individual's legitimate tradeline by becoming an "authorized user," boosting their own credit report with the seller's ostensibly better credit score and better-seasoned, higher-limit account.

This practice, known as "piggybacking," is a significant challenge for financial institutions. While not technically illegal and not always done for nefarious reasons, it frequently manifests as a type of deliberate first-party fraud that distorts the true creditworthiness of a potential borrower. The result is that it's harder to accurately price for risk, along with fueling synthetic identities and leading to higher losses from charge-offs.

While not technically illegal and not always done for nefarious reasons, [purchasing a tradeline] frequently manifests as a type of deliberate first-party fraud that distorts the true creditworthiness of a potential borrower. The result is that it's harder to accurately price for risk, along with fueling synthetic identities and leading to higher losses from charge-offs.



ABUSING A REGULATORY FIX

Piggybacking is rooted in well-intended regulatory action from a bygone era. In 1975, the Federal Reserve promulgated its final rule implementing the Equal Credit Opportunity Act, commonly known as Regulation B.

In Reg B, the Fed addressed a shortcoming of the credit reporting system of the early 1970s, which generally only reported a married couple's credit accounts on the credit report of the husband,



including those jointly held by both husband and wife. As a result, when couples divorced, the woman was left with little credit history of her own.

The Fed sought to rectify this issue by ensuring that a spouse who is only authorized to use an account—rather than being obligated to repay it—should not be put at such a disadvantage, stating: "... [A] spouse who is permitted to use an account shall have the benefit, or burden, of the credit history of that obligation."

That approach has since been clarified and expanded: "[I]f the creditor allows the designation of spouses as authorized users, the creditor may not refuse to accept a non-spouse as an authorized user." This regulatory blessing granted abusive forms of piggybacking an imprimatur of legitimacy, requiring creditors to effectively turn a blind eye to most authorized-user applications.

Pricing risk: Like the first-party-fraud practice of credit washing, abusive piggybacking is designed to hide a borrower's true creditworthiness and risk from a financial institution. Buying access to a better tradeline gives the purchaser's credit a boost, potentially elevating their credit score into a higher band.

Thus, an applicant who would otherwise receive subprime pricing may instead get a prime-rated offer. A lender's risk models rely on the integrity of credit scores and credit reports to paint an accurate picture of a consumer's potential risk. While risk appetites vary from one institution to another, there is understandably no tolerance for credit profiles manipulated by abusive piggybacking.

Synthetic identities: A synthetic identity is created when someone applies for a financial product using a fabricated combination of a name, date of birth and Social Security number. This process triggers the creation of a credit report based on the made-up personally identifiable information.

Left in this state, a synthetic identity isn't of much value. To leverage a fake credit identity to eventually obtain credit and bust out, a fraudster needs to develop the synthetic ID into a reasonably attractive profile. The easiest way to accomplish this is to purchase an authorized user tradeline. In fact, at SentiLink, we observe that about 50% of synthetic identities have at least one authorized user tradeline associated with their credit reports.

Increased charge-offs: Credit extended to an abusive piggybacker masking their true credit profile distorts a lender's ability to manage risk. This is certainly cause for concern; in fact, our analysis suggests authorized user tradelines account for an outsize proportion of poorly performing accounts and losses from charge-offs.

Our research shows that this is reflected across different product verticals. For example, looking at auto loans, we found that roughly 1.5% of past-due balances and nearly 2% of charged-off balances were in piggybacked accounts. For credit cards, the corresponding figures were 1.2% and 1.4%.

Overall, our analysis indicated that, while 0.07% of credit reports were flagged as authorized user tradeline purchasers, these purchasers account for 1% of past-due balances and 1.3% of dollar losses from charge-offs—disproportional effects of 15X and 20X, respectively, and nearly 7X that of a consumer who has not purchased an authorized user tradeline.

A lender's risk models rely on the integrity of credit scores and credit reports to paint an accurate picture of a consumer's potential risk. While risk appetites vary from one institution to another, there is understandably no tolerance for credit profiles manipulated by abusive piggybacking.

HOW TO ADDRESS THE ISSUE

Financial institutions seeking to mitigate abusive piggybacking frequently encounter competing internal challenges. Product and marketing teams see the significant revenue potential of extending credit to more legitimate authorized users; compliance teams feel hamstrung by the "it's fraud, but it's also legal" nature of this problem; and credit-loss teams see the threat but have limited ability to directly stop it.



The best approaches, therefore, are more indirect.

First, when this type of fraud is suspected at scale, focus more resources on identifying synthetic identities at the point of application. As discussed above, fraudsters often buy authorized user tradelines to enhance the credit appearance of a synthetic identity. Employing better tools to flag and stop these identities early can help stop abusive piggybacking.

And when specific cases of abusive piggybacking are suspected, consider a step-up strategy such as income verification. We have seen strong anecdotal evidence that abusive piggybackers are more likely to inflate annual income in disclosures. Tools such as the 4506-C income verification process with the Internal Revenue Service can help prevent scams by creating friction for would-be fraudsters and sending helpful signals to dubious lenders.

These strategies can help financial institutions avoid potential Reg B concerns while enhancing their fraud-fighting toolkits. The legality of abusive piggybacking is not likely to change anytime soon, so innovative approaches are essential to filter out fraudsters from those pursuing authorized user tradelines for legitimate means.

Jason Kratovil is head of public policy and external affairs at SentiLink.

Want to Lower Fraud Losses?

Partner with the Experts in Identity

- Stop more identity fraud and approve more good customers faster.
- Protect against current and emerging fraud trends with a data science-led partner.
- Add technical and human muscle to your fraud and IDV capabilities.
- Free retro study to size your opportunity.

SentiLink

Learn more sentilink.com

Protection from check fraud in a digital world

High-tech printers, specialized ink and other advances can add security to a payment method still embraced by many businesses of all sizes.

BY NATHAN HOLSTEIN

Business processes are rapidly changing around the world. At the same time, millennials and Gen Zers are taking on more prominent roles in private businesses and financial institutions, or opening their own. These younger generations are more comfortable using digital payment apps like Venmo and PayPal, and these apps are easy to access and use. These factors have resulted in a dramatic shift in the way payments are made and accelerated the business world's adoption of more robust digital payment applications.

Against this backdrop, the printed check might seem headed for almost certain obsolescence, but nothing could be further from the truth. Businesses of all sizes still rely on checks as a primary form





The most common method [of check fraud] is alteration of the physical check, which typically involves check washing—the removal of a printed character with a common solvent, such as acetone—or check scraping, the removal of a printed character by carefully scraping the ink or toner with a sharp object or lifting it off with tape.

of payment. The shift in focus to digital payments has helped make checks prime targets for fraud by overshadowing the continued reliance on them.

Deterrents that guard against physical forgery and alteration can add necessary security to printed checks, but businesses often overlook their older printers as significant security vulnerabilities in the check-printing process. Many check printers in use today run firmware that is obsolete and unsupported, creating significant risk for data theft or alteration as checks are printed.

IGNORING CHECKS LEAVES CUSTOMERS VULNERABLE

The digital payments market is expected to grow at a 19.4% compounded annual rate globally through 2028. This growth is primarily attributed to the ever-increasing availability of digital payment services, along with increased smartphone, internet and e-commerce use due to the COVID-19 pandemic.

However, 33% of B2B payments are still being made by check as their primary method of payment. As such, financial institutions need to take a proactive approach to securing their entire check-printing process. Updating often-overlooked network security vulnerabilities such as keeping printers and firmware up to date is one way to reduce fraud risks.

Check fraud remains among the top forms of payment fraud, alongside credit card fraud, ACH fraud and wire fraud. Since 2020, 66% of all companies have experienced actual or attempted check fraud. While check fraud has been decreasing over the past few years, drastic or sudden changes in processes, such as those initiated by the pandemic, have created new vulnerabilities that criminals will exploit once they discover them.

Most people think banks are ultimately liable for any losses, but revisions in the Uniform Commercial Code have shifted liability from the bank to the party in the best position to prevent the loss. In other words, losses are shared between a bank and its customer based upon each party's comparative negligence. Along with the monetary loss, any type of fraud can also cause serious harm to a bank or company's reputation.

HOW DO YOU PROTECT YOUR CUSTOMERS?

Staying up to date on payment security is the best way to protect your business and customers from fraud. A few basic questions can determine your payment security: Do you know how check fraud is committed? What measures are in place to ensure the security of customer transactions?

The first step toward check fraud protection is to become familiar with the methods used in check fraud. The most common method is alteration of the physical check, which typically involves check washing—the removal of a printed character with a common solvent, such as acetone—or check scraping, the removal of a printed character by carefully scraping the ink or toner with a sharp object or lifting it off with tape. Once the payee or amount has been removed, the check is simply reprinted with the fraudulent information.

Once you understand how criminals commit check fraud, there are steps you can take to protect your checks from fraud. MICR printers ensure that printed checks meet all financial industry standards, but some also have built-in network security features that can reduce vulnerability to fraud. For example, some printers have advanced features that prevent unauthorized access to MICR print functions, signatures and form overlays, or that protect the data stream while it is being transmitted.

In addition to making security enhancements to printer firmware, a high-quality MICR toner can help ensure proper character density. This not only reduces the chance of scanning errors and returned checks but also includes modified adhesion characteristics, which guard against scraping. MICR toner is available with incorporated red dye, which releases a stain onto the check if chemical washing is attempted.



A secure numeric font should be used as an added layer of security on the MICR check. This type of font is difficult to alter because it has unique characteristics, such as special backgrounds, texts and numeric elements that are printed in the amount line of the check.

You will also need to verify that the MICR toner and paper you use to print official checks work in unison and provide superior adhesion. The highest level of protection against mechanical alteration is the use of "indelible" printing, a process in which the printed characters permeate the document, preventing the character from being removed without destroying the check. Best-practice MICR check printing also uses blank-check stock rather than stock with a preprinted MICR line to keep valuable information such as account and routing numbers secure until the check is printed.

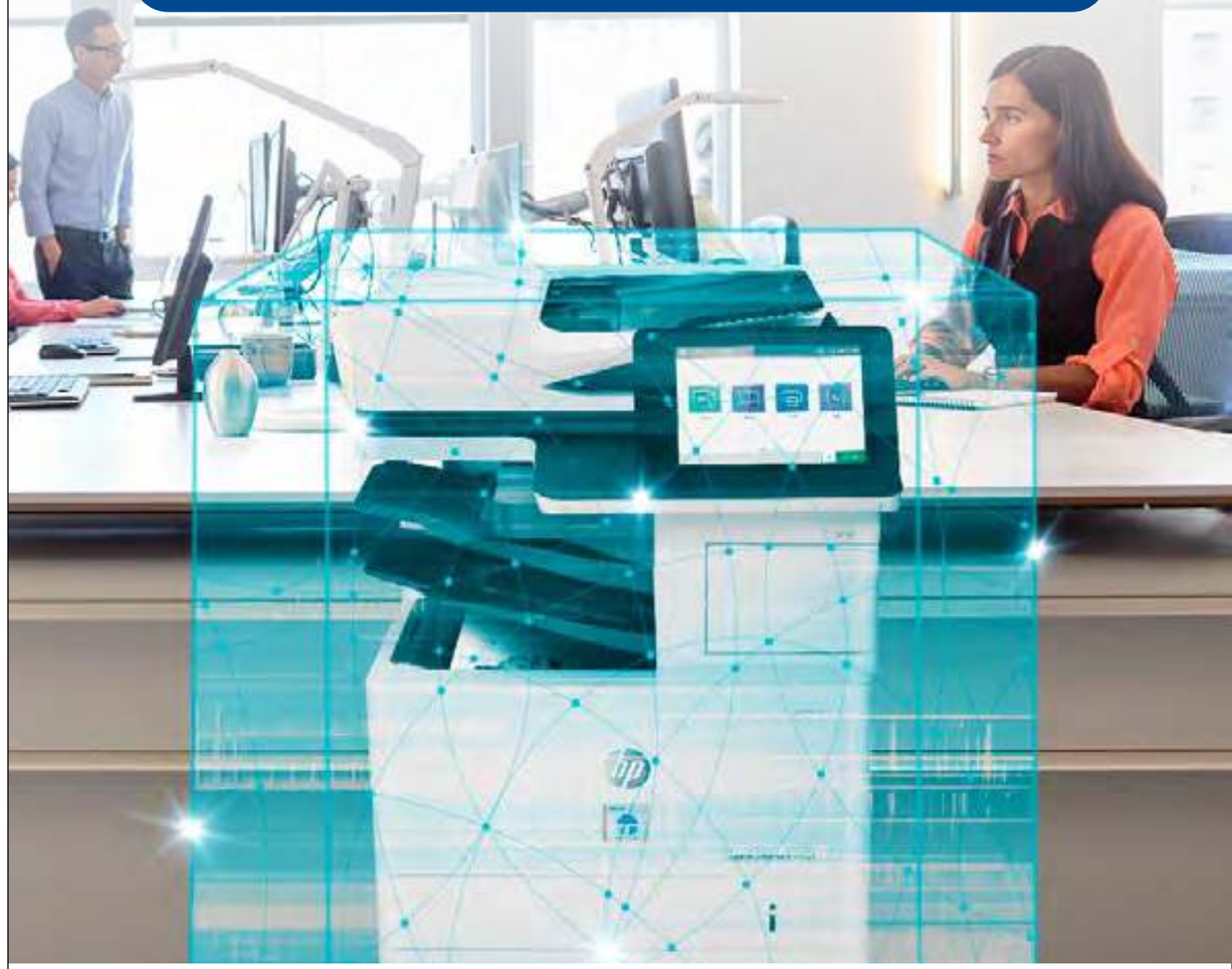
Security fonts are another key element in fraud mitigation. A secure numeric font should be used as an added layer of security on the MICR check. This type of font is difficult to alter because it has unique characteristics, such as special backgrounds, texts and numeric elements that are printed in the amount line of the check. A microprint font adds yet another layer of security on the printed check. The extremely small font embeds personalized microtext and numbers into each check. Designed specifically to work with MICR-specific printers, these fonts are not readily available online and are extremely difficult to forge.

Digital transactions are clearly the future of payments, but they have not eliminated other forms just yet. Checks and other physical forms of payments are still essential for daily transactions and are not going away. Financial institutions should not lose sight of the volume of payments these types represent and should consider taking steps to protect themselves from fraud.

Nathan Holstein is marketing manager for TROY Group.

Are Fraudsters Targeting Your Vulnerabilities?

OUTDATED FIRMWARE LEAVES YOUR BANK OPEN TO FRAUD



Serving the financial services industry with **fraud prevention solutions for printed checks and other vital documents**

304-232-0899 | TROYgroup.com | Secure@TROYgroup.com

TROY®

Past Issues

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? »

AUGUST 2022
Technology is pushing lending in new directions »

STAY TUNED FOR

FEBRUARY 2023
Payments modernization

MARCH 2023
Bank branch outlook

BAI Banking Strategies
EXECUTIVE REPORT

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

JANUARY 2023

BAI POWERING SMART DECISIONS.